QTS Realty Trust, Inc.

Report on QTS Realty Trust, Inc.'s Description of its Information Technology General Control System for Custom Data Center and Colocation services and on the Suitability of the Design and Operating Effectiveness of Controls to Meet the Criteria for the Security, Availability, and Confidentiality Trust Services Principles SOC 2^{SM} Type II

For the period October 1, 2016 to
September 30, 2017

kpmg.com

Contents

© 2017 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. NDPPS 720724

The KPMG name and logo are registered trademarks or trademarks of KPMG International.

Section I - Independent service auditors' report provided by KPMG LLP

KPMG

KPMG LLP
Suite 1100
1000 Walnut Street
Kansas City, MO 64106-2162

Independent Service Auditors’ Report

The Executive Management of QTS Realty Trust, Inc.
QTS Realty Trust, Inc.:

Scope

We have examined QTS Realty Trust, Inc.’s (QTS) description of its system entitled “QTS’s description of its information technology general control system for custom data center and colocation services” for the period October 1, 2016 to September 30, 2017” (the description) and the suitability of the design and operating effectiveness of controls to meet the criteria for the security, availability, and confidentiality principles set forth in TSP section 100A, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Technical Practice Aids)* (applicable trust services criteria), throughout the period October 1, 2016, to September 30, 2017.

The information included in section V, "Other Information Provided by QTS That is not covered by the service auditor's report", is presented by management of QTS to provide additional information and is not a part of QTS’s description of its information technology general control system for custom data center and colocation services system made available to user entities during the period October 1, 2016, to September 30, 2017. Information about QTS's additional service lines and management’s response to exceptions noted has not been subjected to the procedures applied in the examination of the information technology general control system for custom data center and colocation services and the suitability of the design and operating effectiveness of controls to meet the related criteria stated in the description of the information technology general control system for custom data center and colocation services and, accordingly, we express no opinion on it.

QTS uses subservice organizations Iron Mountain, to perform offsite data backup retention and Alert Logic, for performance of periodic vulnerability assessments and intrusion detection security monitoring. The description includes only the controls of QTS and excludes the controls of the subservice organizations. The description also indicates that certain applicable trust services criteria can be met only if complementary subservice organization controls assumed in the design of QTS’s controls are suitably designed and operating effectively, alone or in combination with the related controls at QTS. Our examination did not extend to controls of the subservice organizations and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that certain applicable trust services criteria stated in the description can be achieved only if complementary user-entity controls assumed in the design of QTS’s controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service organization's responsibilities

In section III, QTS has provided an assertion about the fairness of the presentation of the description based on the description criteria and suitability of the design and operating effectiveness of the controls to meet the applicable trust services criteria. QTS is responsible for preparing the description and its assertion, including the completeness, accuracy, and method of presentation of the description and assertion, providing the services covered by the description; identifying the risks that would prevent the applicable trust services criteria from being met; designing, implementing, and documenting controls that are suitably designed and operating effectively to meet the applicable trust services criteria stated in the description.

Service auditor's responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to meet the applicable trust services criteria stated in the description, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of CPAs. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, the description is fairly presented based on the description criteria, and the controls were suitably designed and operating effectively to meet the applicable trust services criteria throughout the period October 1, 2016 to September 30, 2017. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls to meet the applicable trust services criteria involves:

- performing procedures to obtain evidence about the fairness of the presentation of the description based on the description criteria, and the suitability of the design and operating effectiveness of the controls to meet the applicable trust services criteria stated in the description;

- assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to meet the applicable trust services criteria stated in the description;

- testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the applicable trust services criteria stated in the description were met; and

- evaluating the overall presentation of the description.

Inherent limitations

Because of their nature, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to meet the applicable trust services criteria is subject to the risks that the system may change or that controls at a service organization may become ineffective.

Description of tests of controls

The specific controls tested and the nature, timing, and results of those tests are listed in section IV.

Opinion

In our opinion, in all material respects, based on the description criteria and the applicable trust services criteria identified in QTS’s assertion

a. The description fairly presents the information technology general control system for custom data center and colocation services that was designed and implemented throughout the period October 1, 2016, to September 30, 2017.

b. The controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively throughout the period October 1, 2016, to September 30, 2017, and user entities applied the complementary controls assumed in the design of QTS's controls throughout the period October 1, 2016, to September 30, 2017; and

c. The controls stated in the description operated effectively to provide reasonable assurance that the applicable trust services criteria were met throughout the period October 1, 2016, to September 30, 2017 if complementary user entity controls, assumed in the design of QTS's controls, operated effectively throughout the period October 1, 2016, to September 30, 2017.

Restricted Use

This report, including the description of tests of controls and results thereof in section IV, is intended solely for the information and use of management of QTS, user entities of QTS’s information technology general control system for custom data center and colocation services system during some or all of the period October 1, 2016, to September 30, 2017, and the independent auditors and practitioners providing services to such user entities who have a sufficient knowledge and understanding of the following:

— The nature of the service provided by the service organization

— How the service organization's system interacts with user entities, subservice organizations, and other parties

— Internal control and its limitations

— User entity responsibilities, complementary user-entity controls and how they interact with related controls at the service organization to meet the applicable trust services criteria

— The applicable trust services criteria

— The risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks

This report is not intended to be and should not be used by anyone other than these specified parties.

**Note: The locations in scope for this report are Atlanta, Georgia; Chicago, Illinois; Dallas-Irving, Texas; Dulles, Virginia (IAD1 and IAD2); Jersey City, New Jersey; Miami, Florida; Overland Park, Kansas; Piscataway, New Jersey; Richmond, Virginia; Sacramento, California; Santa Clara, California; and Suwanee, Georgia.*

KPMG LLP

October 31, 2017
Kansas City, Missouri

Section II - QTS Realty Trust Inc.’s Assertion

We have prepared the description of QTS Realty Trust, Inc.'s (QTS) system entitled, "QTS's description of its information technology general control system for custom data center and colocation services" for the period October 1, 2016 to September 30, 2017 (the description), based on the criteria in items (a)(i)–(ii) below, which are the criteria for a description of a service organization's system in paragraph 1.26 of the AICPA Guide Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2) (description criteria). The description is intended to provide users with information about the Information Technology General Control System for custom data center and colocation services, particularly system controls intended to meet the criteria for the security, availability, and confidentiality principles set forth in TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Principles and Criteria)* (applicable trust services criteria).

QTS uses subservice organizations to perform offsite data backup retention, periodic vulnerability assessments and intrusion detection security monitoring. The description includes only the controls of QTS and excludes the controls of the subservice organizations. The description also indicates that certain applicable trust services criteria can be met only if complementary subservice organization controls assumed in the design of QTS's controls are suitably designed and operating effectively, alone or in combination with the related controls at QTS. The description does not extend to controls of the subservice organizations.

The description indicates that certain applicable trust services criteria stated in the description can be achieved only if complementary user entity controls assumed in the design of QTS's controls are suitably designed and operating effectively, along with related controls at QTS. The description does not extend to controls of the user entities.

We confirm, to the best of our knowledge and belief, that

a. The description fairly presents the information technology general control system for custom data center and colocation services made available to user entities of the system during some or all of the period October 1, 2016 to September 30, 2017, based on the following description criteria:

   i. The description contains the following information:

      (1) The types of services provided

      (2) The components of the system used to provide the services, which are as follows:

         — *Infrastructure.* The physical structures, IT, and other hardware (for example, facilities, computers, equipment, mobile devices, and other telecommunications networks).

         — *Software*. The application programs and IT system software that supports application programs (operating systems, middleware, and utilities).

         — *People.* The personnel involved in the governance, operation, and use of a system (developers, operators, entity users, vendor personnel, and managers).

         — *Procedures.* The automated and manual procedures.

         — *Data.* Transaction streams, files, databases, tables, and output used or processed by the system.

(3) The boundaries or aspects of the system covered by the description

(4) For information provided to, or received from, subservice organizations or other parties

— How the information is provided or received and the role of the subservice organizations and other parties

— The procedures the service organization performs to determine that such information and its processing, maintenance, and storage are subject to appropriate controls

(5) The applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, the following:

— Complementary user entity controls contemplated in the design of the service organization's system

— When the inclusive method is used to present a subservice organization, controls at the subservice organization

(6) If the service organization presents the subservice organization using the carve-out method

— The nature of the services provided by the subservice organization

— Each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at the service organization, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria

(7) Any applicable trust services criteria that are not addressed by a control at the service organization or a subservice organization and the reasons

(8) In the case of a type 2 report, relevant details of changes to the service organization's system during the specified period covered by the description

ii. The description does not omit or distort information relevant to the service organization's system while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual report user may consider important to its own particular needs.

b. The controls stated in the description were suitably designed throughout the period October 1, 2016 to September 30, 2017 to meet the applicable trust services criteria if the controls operated effectively throughout the period October 1, 2016 to September 30, 2017 and the user entities applied the complementary controls assumed in the design of QTS’s controls throughout the period October 1, 2016 to September 30, 2017.

c. The controls stated in the description operated effectively throughout the period October 1, 2016 to September 30, 2017 to meet the applicable trust services criteria if user entity controls, assumed in the design of QTS's controls, operated effectively throughout the period October 1, 2016 to September 30, 2017.

QTS Realty Trust, Inc.

QTS | Quality Technology Services

DocuSigned by:

Shirley E. Goza

A69AA0FBDA474C5...

[Signature]

General Counsel

[Title]

October 31, 2017

Section III – QTS's description of its information technology general controls system for custom data center and colocation services

Throughout the period October 1, 2016 to September 30, 2017

Company and services overview

QTS is a full-service technology infrastructure company providing data center products, including Custom Data Center and Colocation Services. QTS' systems, infrastructure and experienced staff enable customers to leverage the organization’s economies of scale when outsourcing core components of their IT infrastructure. QTS is headquartered in Overland Park, Kansas with data center facilities located in Atlanta, Georgia; Chicago, Illinois; Dallas-Irving, Texas; Dulles, Virginia (IAD1 and IAD2); Jersey City, New Jersey; Miami, Florida; Piscataway, New Jersey; Richmond, Virginia; Sacramento, California; Santa Clara, California; and Suwanee, Georgia. These locations are included in the scope of this SOC 2 report. QTS continues to invest in data centers and leading technologies to provide availability, security, and capacity for its customers.

Chart of in scope QTS data centers

QTS Data Centers												
Data Center Name	Atlanta Metro	Chicago	Dallas-Irving	Dulles	Jersey City	Miami	Overland Park	Piscataway	Richmond	Sacramento	Santa Clara	Suwanee
Data Center State	Georgia	Illinois	Texas	Virginia	New Jersey	Florida	Kansas	New Jersey	Virginia	California	California	Georgia
Data Center Abbreviation	ATL	CHI	DFW	IAD 1 & IAD 2	JCY	MIA	OVP	PNJ	RIC	SAC	SJC	SUW

Services

QTS' major services consist of offerings designed to meet technology requirements for multiple types of customers. The scope of this report covers Custom Data Center "C1" and Co-location "C2" products as described below. This portfolio enables customers to rapidly respond to changing business application requirements by taking advantage of QTS data centers scale and operations. Other Managed Services "C3" QTS products are described in Section V, "Other Information Provided by QTS that is not covered by the service auditor's report."

C1 – Custom data center

QTS provides Custom Data Centers which can be described as a Data Center within a Data Center. These provide large, private spaces with scalable metered power configurations that are designed, built, and implemented to the customer's specific requirements. Additionally, the customer is able to leverage QTS facilities that provide high-speed Internet connections, security systems and procedures, fully redundant power, and cooling and environmental systems.

C2 – Colocation

QTS provides colocation datacenters within which customers can rent space for servers and other computing hardware. QTS' data centers provide customers with access to facilities that provide multiple, redundant and diverse high-speed Internet connections with security systems and procedures. Additionally, fully redundant power, cooling and environmental systems are in place to maintain the security and safety of customer data. QTS provides standard and customizable options for space on the data center floor in the form of cabinets, cages, and suites. Cabinets are designed to incorporate efficiency, safety, and scalability. Additionally, cabinets are secured with combination locks, electronic badge readers, or biometric readers. Cages are designed for convenience and flexibility of open floor space. Cages are secured with key locks or electronic badge readers and can accommodate open racks, cabinets and free-standing or non-rack-mountable equipment. For customers requiring a higher level of security or large amounts of floor space, suites made of solid wall structures are available. These structures restrict visibility, are secured with electronic badge readers or biometric readers and also can incorporate secure enclosures across the top of the suite and below the floor.

Components of the system

The components of QTS' information technology general controls system for C1 – Custom Data Center Services and C2 – Colocation Services that are included in the scope of this report are included in the sections below.

Infrastructure

The QTS infrastructure system includes physical and hardware components such as facilities, equipment and networks. The data center facilities include custom data center and colocation services listed in the services overview section. QTS provides standard and customizable options for space on the data center floor in the form of cabinets, cages, and suites. Cages can accommodate open racks, cabinets and free-standing or non-rack mountable equipment. Custom data center suites are made of solid wall structures and can incorporate secure enclosures across the top of the suite and below the floor. To support the facilities operations, QTS utilizes environmental, electrical power & cooling, physical & technology hardware, redundancy, and internal and external security equipment. QTS manages and is responsible for the feed of electrical power up through QTS' owned infrastructure. QTS uses the hardware components to comprise the systems that provide services to customers and the infrastructure to support QTS' customers.

Software

QTS utilizes programs and operating software to manage business functions such as network-based and host-based intrusion detection services, backup and storage management, storage array management, system administration, antivirus, monitoring, access policy management, network management, incident management, system development and change management, access control, physical security, environment security, patch and maintenance identification. The systems in scope for this report are the internal systems that support QTS's operations. Logical access, including provisioning and deprovisioning, to these programs and software is managed through a homogenous process.

Name	Description	Locations
Jump, Compliance and Dulles Domain (Jump/Comp/Dulles)	The QTS "Jump", "Compliance" and "Dulles" domains are Active Directory domains that employees authenticate to before accessing the in-scope systems listed below.	All
Lenel	Lenel is the physical access system that is used to monitor physical access and provides physical badge access for QTS' Data Center facilities.	DFW, PNJ, RIC
Prowatch	Prowatch is the physical access system that is used to monitor physical access and provides physical badge access for QTS' Data Center facilities.	ATL, CHI, IAD1, IAD 2, JCY, MIA, OVP, SAC, SJC, SUW
PELCO	PELCO is the video surveillance system for the QTS IAD 1 Data Center facility.	IAD 1

Name	Description	Locations
Genetec	Genetec is the video surveillance system for QTS' Data Center facilities.	ATL, CHI, DFW, IAD 2, JCY, MIA, OVP, PNJ, RIC, SAC, SJC, SUW
ServiceNow	ServiceNow is used for internal and customer workflow tickets.	All
Andover Continuum	Andover Continuum provides the Power monitoring for QTS' Data Center facilities.	ATL, DFW, IAD 1, IAD 2, JCY, MIA, OVP, SJC, SUW
Wonderware	Wonderware provides the Power Monitoring for QTS Data Center facilities.	ATL, IAD 1, IAD 2, PNJ, RIC, SAC, SJC, SUW
Siemens	Siemens provides the Power Monitoring for QTS' Data Center facilities.	CHI & DFW
CA Unified Infrastructure Management (CAUIM)	CAUIM is the availability monitoring tool.	All
Patchlink	Patchlink automatically identifies new releases from Microsoft and sends notifications to the Operations Service Center ("OSC") for the specific servers applicable to receive the new releases.	All
Netbackup	Symantec NetBackup provides a complete, flexible data protection solution for a variety of platforms. NetBackup allows back up, archive, and restore files, folders or directories, and volumes or partitions.	All
Unisphere	The EMC Unisphere Console is utilizes a web based portal for Storage Array management.	All
AlertLogic	AlertLogic is a vendor solution that provides an intrusion detection system (IDS) and vulnerability assessment solution.	All
Cisco AnyConnect VPN Client/Server	VPN Remote access system for the enterprise.	All
Juniper	Intrusion detection system (IDS) and VPN Remote access system for the enterprise.	IAD 1 & IAD 2
Junos	Junos is an operating system that is used in Juniper's routing, switching and security devices.	IAD 1 & IAD 2
ScreenOS	ScreenOS is a real-time embedded operating system for the NetScreen range of hardware firewall devices from Juniper Networks.	IAD 1 & IAD 2

Name	Description	Locations
Aptare	Aptare is the tool that schedules backups on customer systems and also monitors the results of the backup jobs and reports on the results.	All
Splunk	Splunk is a tool used to capture application version change logs.	All
Symantec Endpoint Protection (SEP)	Anti-Virus and IPS Solution.	All
Window and Unix Servers (physical and virtual)	Servers that help support the overall IT infrastructure of QTS.	All
TPC Online and Absorb	TPC Online and Absorb are the interactive maintenance training solutions with training catalogs across many industries.	All
Phone Factor	The Phone Factor Application is the 2 factor authentication that supports the Jump and Compliance Domains within the QTS network environment.	ATL, CHI, DFW, JCY, MIA, OVP, PNJ, RIC, SAC, SJC, SUW
RSA	The RSA Application is the 2 factor authentication that supports the Dulles Domain within the QTS environment.	IAD 1 & IAD 2
EMaint	EMaint is a Computerized Maintenance Management Software and helps manage maintenance operations.	All
SecureAdmin	SecureAdmin is the Biometric reader that ensures limitations around physical access to QTS sites.	DFW, MIA, OVP, RIC, SAC
VeriAdmin	VeriAdmin is the Biometric reader that ensures limitations around physical access to QTS sites.	ATL, JCY, SJC, SUW
Bioscrypt	Bioscrypt is the Biometric reader that ensures limitations around physical access to the QTS' sites.	IAD 1, IAD 2, PNJ

People

QTS' Board, Audit Committee, Internal Audit and executive management designate the appropriate levels of responsibility and authority to ensure internal controls are operating effectively. The Board, Audit Committee, and any applicable sub-committees have been provided proper authorization via designated charters. Executive and senior management are responsible for verifying that employees understand the regulations and adhere to the internal controls, policies and procedures. Two key functions in delivering services and adhering to the policies and procedures are the Operations and Product Development groups.

Operations

This division is responsible for the daily functional aspects of information technology which includes the physical and environmental infrastructures and vital data center operations. Technical engineers at each data center ensure hardware infrastructure and any other computer related needs. Management is aware of the risks attributed to the IT infrastructure such as security and disaster recovery and their effects on the organization as a whole. Operations employees are trained in industry security practices and are continuously learning about and monitoring the security infrastructure of the organization.

Product development

This division is instrumental in researching, developing, and building solutions to be used for individual customer needs. Individuals within this division maintain contact with QTS' customers for the purpose of obtaining information needed to foster a harmonious working environment between both parties and to develop a concrete platform regarding the applicable software and hardware needs for each customer's respective solutions.

For additional information on organizational management including hiring practices, reporting relationships and job responsibilities, refer to the *Organization and Administration section.*

Procedures

QTS has documented policies and procedures in place for the information technology general controls over core infrastructure and managed services. These procedures include:

- Logical and physical security
- System development and change management
- Backup and recovery
- Data center operations
- Disaster recovery planning and business continuity
- Policy management and communication
- Data encryption

Additionally, customer changes impacting existing systems and hardware must be approved by QTS management and must align with technology requirements.

The Corporate Policy Board Committee ("CPB") oversees the development and distribution of policies and procedures. It consists of Line of Business ("LOB") owners across the organization and is chaired by a member of the Compliance department. The CPB meets on a quarterly basis, or more frequently as required, to review and approve new corporate wide policies and procedures. Additionally, the CPB verifies that policy owners review QTS policies on an annual basis. Approved CPB policies are communicated to QTS employees via e-mail and are made available within the company's document repository tool.

Data

QTS may come into contact with data provided by customers during provision of its services. QTS considers all removable backup media as confidential and encrypts backup media. Additionally, QTS obtains confidentiality commitments within formal information sharing agreements with related parties and vendors such as non-disclosure agreements (NDA), Master Agreements of Professional Services and customer Master Service Agreements. As a part of the provisioning process, QTS' obligations and commitments are established including handling of data and maintaining the data's confidentiality.

The system also includes data residing in QTS systems that govern QTS processing and controls. Customer data residing in customer systems and networks is not part of the system covered by this report.

Information and technology general control
System operations

Organization and administration

QTS has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system. HR generates and updates organizational charts as necessary. As changes are required, QTS management will approve reporting relationships on the organizational chart. Additionally, QTS has written job descriptions specifying the responsibilities and academic and professional requirements for key job positions. The written job descriptions will include individuals who are responsible for the design, development, implementation, and operation of systems affecting security, availability and/or confidentiality. Job descriptions are reviewed and updated as necessary by HR. Hiring procedures include a comprehensive screening of candidates for key positions and consideration of whether the candidate’s credentials are commensurate with the position's defined responsibilities.

Prospective employees are required to undergo background checks, drug screening and credit checks prior to employment. QTS sends the applicant a background screening authorization form and once the applicant provides his/her authorization, HR sends a second group of documents to the prospective employee. Information received from the background check including criminal convictions is reviewed and considered in making the decision to hire the applicant. If QTS extends an offer of employment, the individual is required to sign a NDA and/or confidentiality agreement within 10 days of the first day of employment. Once the applicant is hired by QTS, the employee handbook is provided to the new employee who is required to certify acknowledgement via electronic signature. Employee handbook policies are communicated to current QTS employees annually and whenever updated.

To keep employees informed of trends in information security, QTS provides updated policies and procedures, which include security incident response. These policies and procedures are posted within the entity’s document repository tool.

Additionally, QTS has documented policies, procedures, descriptions of the organization structure, processes, and organizational roles & responsibilities which are posted on the entity’s intranet made available to internal users. The description delineates the parties responsible, accountable, consented, and informed of changes in design and operation of key system components. Employees are required to complete an annual security awareness training facilitated by the Information Security Office (“ISO”). The security awareness training informs employees about the company's security, availability and confidentiality commitments and the process for identifying and reporting possible system availability issues, security breaches, confidentiality breaches, and other incidents. QTS has a specific training department who manages online training and leads training efforts. As a part of the annual budget process, each department is assigned a training budget to fulfill their specialized training needs.

QTS maintains a line of communication with customers from the provisioning process (at which point they are set up) through continued support of on-going operations. As a part of the provisioning process, QTS’ obligations and commitments are established including handling of data and maintaining the data’s confidentiality. QTS also communicates the procedures for handling operational failures, incidents, problems, concerns and complaints to customers and how customers can alert QTS of any issues with their applicable systems. QTS has prepared and posted to the internet a description of its products and services and the acceptable use policy for external users. System descriptions are available to authorized external users that delineate the boundaries of the system via ongoing communications with customers or via the customer portal. Once the customer indicates a system incident has occurred, the Operations Service Center (OSC) executes the incident response process to correct the issue. Furthermore, QTS's security, availability, and confidentiality commitments regarding the system are included in the master space agreements, leases and customer-specific service level agreements. In addition, a summary of these commitments, data center rules and customer responsibilities are available on the customer portal.

Operations Service Center ("OSC")

Customers can contact the OSC 24 hours per day, 7 days per week. Requests (also called "tickets") can be submitted by authorized customer contacts via phone, email, or web portal. Customer Support Representatives ("CSRs") receive the customer requests and are recorded as tickets through ServiceNow. Requests may only be processed by customers whose names appear on their respective company's security roster. Before the ticket can be processed, the customer must provide a security pass-phrase to the OSC. This is a word or phrase previously selected by the customer and recorded in ServiceNow. The security roster and pass-phrase assists in preventing unauthorized changes from being made to a customer's equipment or account. Emails sent to the support mailbox automatically generate a ticket which is reviewed by a CSR, who then authenticates the sender with the corresponding customer-provided pass-phrase. The QTS Web portal automatically pre-authenticates the customer's request by utilizing the customer's pass-phrase for a password upon login to the portal.

ServiceNow automatically assigns a priority to each ticket based on impact and urgency parameters ("Priority"). Tickets are addressed in accordance with their Priority; higher Priority tickets are addressed before lower Priority tickets. Once a ticket has been opened, the CSR or an OSC engineer escalates the ticket as necessary. The ticket is initially escalated to the engineers in the OSC. These engineers are trained to perform basic configuration changes and troubleshooting. The ticket is verified and worked by the OSC engineer and is escalated to product-specific engineers as needed.

Incident response

QTS uses internally managed and externally provided software tools and procedures to monitor, report, and manage system availability issues, security breaches, confidentiality breaches, complaints and other incidents. The OSC is generally the first entity involved in the incident response process and is available 24 hours per day, 7 days per week for customers to communicate any system incidents. For major incidents, an After Action report is prepared including a resolution. Based on the resolution, change requests are prepared, controls are evaluated and updated if needed, policies and procedures are updated as needed. The OSC has defined rules for classifying priority of any incident by Impact and Urgency to minimize the impact to customers. The OSC also has detailed procedures to triage, address, and escalate if needed, customer incidents. Any high severity incidents are reviewed with QTS Management and the ISO to assess the root cause of any high severity incidents and verify that appropriate actions are taken to address the root cause of any high severity incidents.

To provide continuous monitoring of the availability of the QTS infrastructure and customer systems, the CAUIM tool is used. Availability monitoring is performed 24 hours per day, 7 days per week by the OSC. If an issue occurs, action is taken by on-call engineers to minimize the impact to customer services. Detailed procedures have been established to assist in the identification, notification and escalation of possible system availability issues.

Throughout the incident management process, notes are recorded in the ticket by individuals who handle the incident; administrative or labor-related actions also are recorded. These notes may be selectively displayed to the customer via the customer web portal. Once resolved, the ticket is marked as "Resolved" in ServiceNow and an automated email is sent notifying the customer. If service has been restored, and/or the customer does not require further action on the ticket, the ticket is marked as "Closed" and another automated email is sent to notify the customer.

Physical security

Physical security procedures are enacted so that only authorized individuals have access to physical locations such as the QTS data center facilities, data center rooms, computer operational centers, electrical/mechanical rooms, and other critical areas. Elements of physical security include exterior and interior security elements, access control elements, electronic access badge administration, and monitoring elements.

Exterior security elements

The QTS data center facilities are equipped with fences and/or walls located around the perimeter of the building which assist in preventing unauthorized access.

The QTS data center facilities are equipped with exterior lighting for visibility outside the facilities during night hours, which assist in preventing potential intruders from approaching the buildings unseen.

Security surveillance cameras are strategically positioned around the exterior of the buildings for monitoring and recording of external building activity. The video is monitored 24x7x365 by the Security Office or OSC where there is no 24x7. Backup is maintained on site for 90 days.

Interior security elements

The QTS data center facilities are manned by security staff 24 hours per day, 7 days per week. Physical security at each data center is managed by a security team comprised of a QTS Security Manager and third party security officers. QTS uses security services organizations for its contracting of third party security officers and these organizations have contractual obligations to perform background checks on the security officers.

The QTS Security Managers maintain oversight to ensure policies and procedures and security rounds are appropriately followed. Security officers perform regularly scheduled rounds daily looking for anything unusual, suspicious, or out of the ordinary. The data center security teams are responsible for a variety of critical activities and functions, including but not limited to:

- Controlling and monitoring data center access, prevention of unauthorized access;
- Verifying compliance with access procedures;
- Controlling the movement of items removed via the facility main entry point;
- Loss prevention;
- Issuance and retrieval of ID access badges;
- Administration of the computerized access control system;
- Administration and maintenance of physical security systems and video surveillance systems;
- Monitoring of, response to, and resolution of security alarms;
- Conducting scheduled and unscheduled security, fire, and safety patrol inspections;
- Enforcement of policy to prevent unauthorized photography;
- Enforcement of policy prohibiting food, drink or cardboard within the data center;
- Escorting visitors without access credentials;

- Assisting customers with cage lockouts; and,
- General compliance with security policies and procedures.

The raised floor data center areas of the facilities are secured with floor tiles made of concrete, and data center entry/exit is not easily accessible from under the raised floor. Cabinets, cages, and suites are constructed of metal and are of appropriate strength and rigidity to secure customer equipment from unauthorized access. Data center cabinets, cages, and suites in the facility are fastened to the floor, are clearly labeled, and are periodically inspected to ensure their proper physical condition. Cabinets, cages and suites are secured with combination locks, traditional lock and key mechanisms, or electronic badge readers depending on access control requirements dictated by customers. Holding rooms are utilized for added data center area security and must be cleared prior to accessing the data center area of the facilities. See chart within this section for the specific security elements in place at each data center.

Access control elements

The QTS data center facilities are equipped with electronic badge reading systems which are managed and maintained by the security teams to prevent unauthorized access to areas within the facilities. Each area of each building is considered a separate security zone and is configured individually within the electronic badge reading system for access to that specific area.

Visitors to the QTS data center facilities are required to have checked in with their official government-issued picture identification, their visit logged by the security team and must be escorted at all times by QTS employees or security officers.

In addition to the electronic badge reading systems, the facilities are equipped with biometric iris scanning devices and biometric fingerprint reading devices in select areas throughout the facilities. Like the electronic badge reading system, each area of the buildings protected by these biometric devices is considered a separate security zone and is configured individually within the systems for access to that specific area. Individuals have their biometric attributes configured in these systems by the security team in accordance with the documented access requirements.

Access to the data center floors is gained by clearing a holding room that requires two-factor authentication. Individuals requiring access to a data center floor first use their electronic access badge and their biometric fingerprint to gain entry to the holding room. Individuals then have their iris scanned by an iris reader inside the holding room to gain access to the data center floor. On a periodic basis, the list of QTS employees and contractors with access to each data center is reviewed as an additional control to confirm processing of user change and de-provisioning requests.

Electronic access badge administration

Access badge provisioning and changes to electronic access badges are performed by the security team under a structured enrollment program which applies to QTS employees, contractors, and customers. For QTS employees and contractors, the process is initiated when the individual's supervisor submits a user provisioning request within ServiceNow for approval to the HR department for physical access. The HR department reviews the request and upon approval, forwards the request to the OSC. The OSC follows the process described in the Support Services section above to validate the individual's authorization. The OSC then opens a ticket and assigns a task to the security team at the specified location(s). Upon receipt of the assigned task, the security team reviews the appropriateness of the request and activates an electronic access badge and assigns the necessary security zones. The type and duration of access is determined based on parameters specified in the access request documented. When the electronic access badge has been assigned, the security team closes the assigned task within the ticket. Once assigned tasks are closed, the ticket is closed by the OSC. For customers, the key customer point of contact submits the request/approval to the QTS Service Account Manager who forwards the request to the OSC. Once the request is received by the OSC, the provisioning follows the same process as QTS employees and contractors.

Electronic access badges are deactivated when the OSC is notified of terminations via a ServiceNow de-provisioning request, requesting the removal of physical access. The OSC validates that the request is from an authorized individual, opens a ticket, and assigns a task to the security team at the specified location(s). Once confirmed the tasks are auto generated to all relevant system administrators for confirmation of removal. Upon receipt of the assigned task, the security team deactivates the electronic access badge. When the electronic access badges are deactivated, the security team closes the assigned task. Once assigned tasks are closed, the ticket is closed in ServiceNow. For customers, the primary customer point of contact submits the request/approval for removal of physical access to the QTS Service Account Manager who forwards the request to the OSC. Once the request is received by the OSC, the de-provisioning follows the same process as QTS employees and contractors. Additionally, badges are set to auto-disable after 180 days of inactivity.

The security teams at each QTS data center facility have administrative access to the electronic badge reading systems (Prowatch and Lenel) which allows them to activate/deactivate electronic access badges and manage/assign security zones. Administrative access to the electronic badge reading systems ("security badging system") is reviewed on a periodic basis by running a system-generated report of individuals with administrative access and distributing the report to the respective LOB owner for their review. LOB owners will identify required changes and generate a ticket for the identified required changes to be made to the listing of individuals with administrative access.

Monitoring elements

The facilities are equipped with fixed position and pan, tilt, zoom ("PTZ") security cameras for video surveillance of critical areas in and around the buildings. The exterior and interior of the buildings are monitored by cameras which are strategically positioned for optimum coverage of critical areas. Images from the security cameras are displayed on monitors maintained in the security room which is accessible only to security officers and are viewed by a member of the security team at times when not engaged in other security duties. Video surveillance streams are recorded to video archive servers. The archive servers are located in a secure area that is only accessible to QTS security personnel and data center technicians. Video archives are maintained for a period of ninety (90) days before they are overwritten, and the entire video surveillance system is protected by an uninterruptable power supply ("UPS") in the event there is a loss of power.

See below for chart that details the specific levels of physical security in place at each in-scope data center.

Physical Security									
Data center	**Data center fence/ walls**	**Data center security guard stands**	**Surveillance cameras**	**Raised data center floors**	**Concrete floor tiles**	**Two-factor authentication holding rooms**	**Metal cabinets, cages and suites**	**Biometric scanning devices (Fingerprint & Iris)**	**Electronic card key readers**
ATL	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes, Both	Yes
CHI	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes, Both	Yes
DFW	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes, Both	Yes

Physical Security									
Data center	Data center fence/ walls	Data center security guard stands	Surveillance cameras	Raised data center floors	Concrete floor tiles	Two-factor authentication holding rooms	Metal cabinets, cages and suites	Biometric scanning devices (Fingerprint & Iris)	Electronic card key readers
Dulles (IAD1 & IAD2)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
JCY	N/A – High Rise Building	Yes	Yes	Yes	Yes	Yes	Yes	Yes, Both	Yes
MIA	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes, Both	Yes
OVP	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes, Both	Yes
PNJ	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes, Both	Yes
RIC	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes, Both	Yes
SAC	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes, Both	Yes
SJC	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes, Both	Yes
SUW	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes, Both	Yes

Environmental security

Environmental security procedures are the measures utilized to protect the facilities from fire, electrical surges, spikes, sags, and outages, as well as mechanical issues that may arise with temperature and humidity maintenance elements. Each data center maintains a critical maintenance plan which is reviewed and updated at least annually or as necessary. The elements of environmental security are comprised of electrical, mechanical, monitoring, and fire prevention systems.

Electrical

Diesel generators at each QTS data center facility provide backup power in the event utility power becomes unavailable. Power for the QTS data center facilities, whether originating from the utility provider or from the backup generator environment, is routed to the UPS environment before delivery to the Power Distribution Units ("PDUs"). The UPS systems are designed to bridge the gap between the utility power and the backup generator power delivery. They condition the power feed and protect data center equipment from spikes or sags in power. The PDUs deliver output power to customer and company infrastructure equipment at the appropriate voltage depending on requirements.

Generators are periodically load-tested and the UPS systems and PDUs are inspected regularly by facilities personnel (see below for processes around monitoring of equipment). Additionally, onsite diesel/fuel is regularly monitored by facilities personnel for availability in the event that the backup generators are required. Generators are supported by on site backup reserve tanks.

Environmental safeguards are implemented throughout the data centers at N+1 redundancy configuration where possible (significant components have at least one independent backup component) to provide for the safety of the employees, company property, and other equipment. At a minimum, all sites have redundancy in place for the generators, UPS and PDU devices. Larger sites are configured to also have N+1 redundancy in place for the power utility feeds and transformers. See below for chart that details the specific levels of electrical environmental security in place at each in-scope data center.

Environmental Security – Electrical						
Data center	**On-site substations**	**Power utility feed**	**Transformers (Redundancy)**	**Generators (Redundancy)**	**UPS Devices (Redundancy)**	**PDU Devices (Redundancy)**
ATL	Yes	Single Feed	Yes (N+1)	Yes (N+1)	Yes (N+1)	Yes (N+1)
CHI	No	Double Feed	Yes (N+1)	Yes (N+1)	Yes (N+1)	Yes (N+1)
DFW	Yes	Double Feed	Yes (N+1)	Yes (N+1)	Yes (N+1)	Yes (N+1)
Dulles (IAD1 & IAD2)	No	Single Feed	No	Yes (N+1)	IAD 1 – Yes (2N) IAD 2 – Yes (N+1)	Yes (N+1)
JCY	No	Double Feed	No	Yes (N+1) Floor 17 (N)	Yes (N+1)	Yes (N+1)
MIA	No	Single Feed	Yes (N+1)	Yes (N+1)	Yes (N+1)	Yes (N+1)
OVP	No	Single Feed	No	Yes (N+1)	Yes (N+1)	Yes (N+1)
PNJ	Yes	Double Feed	Yes (N+1)	Yes (N+1)	Yes (N+1)	Yes (N+1)
RIC	Yes	Single Feed	Yes (2N)	Yes (N+1)	Yes (N+1)	Yes (N+1)
SAC	No	Single Feed	Yes (N+1)	Yes (N+1)	Yes (N+1)	Yes (N+1)
SJC	No	Single Feed	No	Yes (N+1)	Yes (N+1)	Yes (N+1)
SUW	No	Double Feed	Yes (2N)	Yes (N+1)	Yes (N+1)	Yes (N+1)

Mechanical

The QTS data center facilities are equipped with temperature control systems designed to provide cooling and humidity control for the facilities. The systems are configured to deliver consistent air temperature and humidity levels. Persistent deviations from the configured temperature settings and humidity parameters trigger alerts to the monitoring system. The mechanical devices within these systems are regularly monitored and maintained by facilities personnel. The cooling systems are designed with built-in redundancy (N+1 levels or greater). See below for chart that details the specific levels of mechanical environmental security in place at each in-scope data center.

Environmental Security – Mechanical			
Data center	**Chillers (Redundancy)**	**Air conditioner units (Redundancy)**	**CRAC/CRAH units (Redundancy)**
ATL	Yes (N+1)	N/A	Yes (N+1)
CHI	N/A	Yes (N+1)	Yes (N+1)
DFW	Yes (N+1)	N/A	Yes (N+1)
Dulles (IAD1 & IAD2)	IAD 1 – Yes (N+1) IAD 2 – N/A	IAD 1 – N/A IAD 2 – Yes (N+3)	Yes (N+1)
JCY	N/A	Yes (N+1)	Yes (N+1)
MIA	Yes (N+1)	N/A	Yes (N+1)
OVP	N/A	Yes (N+1)	Yes (N+1)
PNJ	Yes (N+1)	Yes (N+1)	Yes (N+1)
RIC	Yes (N+1)	N/A	Yes (N+1)
SAC	Yes (N+1)	N/A	Yes (N+1)
SJC	Yes (N+1)	N/A	Yes (N+1)
SUW	Yes (N+1)	N/A	Yes (N+1)

Monitoring

Monitoring of electrical and mechanical elements at the QTS data center facilities is performed using automated alerts. When an alert is generated by a critical electrical or mechanical element, the systems are configured to send email notifications to electrical and/or mechanical personnel for assessment as well as to notify the OSC where a ticket is created in ServiceNow for tracking purposes. Alerts that require escalation beyond onsite electrical or mechanical personnel are addressed in accordance with the criticality of the alert as dictated by QTS policy.

To provide continuous monitoring of the availability of the QTS infrastructure and customer systems, the CAUIM tool is used. Availability monitoring is performed 24 hours per day, 7 days per week by the OSC. If an issue occurs, action is taken by on-call engineers to minimize the impact to customer services.

Detailed procedures have been established to assist in the identification, notification and escalation of possible system availability issues.

Additionally, electrical and mechanical technicians conduct daily tours and physically inspect significant pieces of equipment. Critical data metrics are recorded and unusual observations or deficiencies are reported and analyzed to identify and address potential equipment failures before they occur.

Fire prevention

A central monitoring control panel is located in the Fire Control Room in each facility that displays the status of various fire elements throughout the facility. The central monitoring control panel aggregates data from several other control panels in various locations of the facility that are tied to their particular elements, and is secured by lock and key with access restricted to authorized personnel only. Monitoring of critical fire elements including fire and smoke detectors, HVAC alarms, water sensors, and annunciators is done within the facility in addition to onsite monitoring efforts undertaken by QTS security personnel.

A wet pipe fire suppression system protects the office and common areas of the facilities, while the data center and other critical infrastructure areas of the facilities are protected by a pre-action dry pipe fire suppression system. The system operates independently in each area of the building so an alert condition that causes the dry pipes to fill in one area of the building does not cause the dry pipes to fill in another area of the building. Additionally, the fire suppression system in the data center areas is enhanced by the implementation of Very Early Smoke Detection Apparatus ("VESDA") where possible, a highly-sensitive type of smoke detector. The VESDA smoke detectors provide enhanced protection from fire conditions by reading air samples with highly sensitive laser technology that detects smoke particulates during the earliest stages of a fire condition. The fire suppression system is inspected annually to validate its proper working condition and compliance with fire codes.

Fire suppression for the transport and battery rooms is provided by an FM 200 system, which is a chemical-based waterless fire suppression system that deploys quickly without leaving behind residue or particulates, and operates independently from the water-based pre-action dry pipe fire suppression system. To aid in the suppression of small incipient fires, fire extinguishers are positioned strategically throughout the facility and are periodically inspected by QTS maintenance personnel as well as an outside vendor to validate their readiness and proper operation.

See below for chart that details the specific levels of fire prevention environmental security in place at each in-scope data center.

Environmental Security – Fire Prevention						
Data center	**Central monitoring control panel**	**Fire and smoke detectors**	**VESDA**	**Data center floor: pre-action dry pipe fire suppression system**	**Data center floor: chemical-based waterless fire suppression system**	**Fire extinguishers**
ATL	Yes	Yes	Yes	Yes	Yes	Yes
CHI	Yes	Yes	Yes	Yes	Yes	Yes
DFW	Yes	Yes	Yes	Yes	Yes	Yes

Environmental Security – Fire Prevention						
Data center	**Central monitoring control panel**	**Fire and smoke detectors**	**VESDA**	**Data center floor: pre-action dry pipe fire suppression system**	**Data center floor: chemical-based waterless fire suppression system**	**Fire extinguishers**
Dulles (IAD1 & IAD2)	Yes	Yes	Yes	Yes	Yes	Yes
JCY	Yes	Yes	Yes, 17th floor only. See the pre-action dry pipe fire suppression system column for the other data center floors	Yes	Yes	Yes
MIA	Yes	Yes	Yes	Yes	Yes	Yes
OVP	Yes	Yes	No, See the pre-action dry pipe fire suppression system column.	Yes	Yes	Yes
PNJ	Yes	Yes	Yes	Yes	Yes	Yes
RIC	Yes	Yes	Yes	Yes	Yes	Yes
SAC	Yes	Yes	Yes	Yes	Yes	Yes
SJC	Yes	Yes	Yes	Yes	Yes	Yes
SUW	Yes	Yes	Yes	Yes	Yes	Yes

Logical security

Logical security is enforced by the process of authentication and authorization practices directly tied to access control lists that define what resources users are permitted to access. This process applies to QTS employees and contractors (personnel) who have access to QTS networks and systems in order to support QTS service delivery. The systems in scope for this report are the internal systems that support QTS's operations.

Windows terminal services

QTS utilizes a Windows Terminal Server for personnel who perform work on customer networks and systems from remote locations. Personnel first authenticate to the QTS "Jump domain", "Compliance domain" or "Dulles domain" before gaining access to customer environments. This provides a clear separation of access between customers who access their systems from their own networks and QTS personnel who access the systems from the QTS Jump or Compliance domain.

Granting access

QTS employees and contractors are assigned appropriate permissions based on their job descriptions and roles/responsibilities within the organization. For QTS employees and contractors, the process is initiated when the individual's supervisor submits a user provisioning request within ServiceNow for approval to the HR department for logical access. The HR department reviews the request and upon providing approval, forwards the request to the OSC. The OSC assigns a task to the Domain/System Administrator. Upon receipt of the assigned task, the Domain/System Administrator creates the user account and/or assigns the necessary permissions based on parameters specified in the access request. When this process is completed, the Domain/System Administrator closes the assigned task. Once assigned tasks are closed, the ticket is closed in ServiceNow.

Removing access

Logical access is removed following a similar process, an employee's or contractor's supervisor or HR completes a user de-provisioning request within ServiceNow. HR reviews the request and transfers it in ServiceNow to the OSC for task assignment to the Domain Administrators. Upon receipt of the assigned task, the Domain Administrator deactivates the user account and/or removes permissions based on parameters specified in the access request. When this process is completed, the Domain Administrator closes the assigned task. Once assigned tasks are closed, the ticket is closed in ServiceNow.

Reviewing access

The Domain Administrators have administrative access to Active Directory which allows them to activate/deactivate user accounts and manage permissions. The Information Security Officer (ISO) at QTS leads a periodic access review. On a periodic basis, user accounts, access control lists, and system and service accounts with elevated privileges are reviewed for appropriateness. The review is executed by running a system – generated report of accounts and the permissions associated with those accounts.

The report is distributed to system owners and LBO owners periodically who review the access listing for appropriateness and document identified discrepancies to the ISO team. A ticket is then opened to communicate the necessary access modifications to the applicable system or applications. Once the access modification request is completed, the access listings are re-run and the ISO team ensures changes have been appropriately processed. The following are additional details of systems which are included in the periodic access reviews:

- Accounts, groups, and access control lists, including Domain Administrators on the Jump, Compliance and Dulles Domains.
- Application accounts with the ability to modify Physical Security.

Password management

Security parameters for user IDs and passwords include the following Active Directory password requirements:

- A temporary password is created for new accounts which must be changed upon initial log-in. User IDs and passwords must meet or exceed network complexity rules, and passwords cannot be common dictionary words or be the same as an employee's user ID;

- The information system enforces a limit of no more than three (3) consecutive invalid access attempts by a user during an organizationally defined time period;
- The information system automatically locks the account/node for a period of thirty (30) minutes, or until an administrator enables the user ID, when the maximum number of unsuccessful attempts is exceeded;
- The information system prevents further access to the system by initiating a session lock after a maximum of fifteen minutes (15) of inactivity;
- User passwords are required to be changed every ninety (90) days; and
- Passwords must be immediately changed if they are suspected of being compromised, disclosed, or known to unauthorized parties.

Network security

Customer access

Access to customer systems is further secured through the implementation of multiple layers of authentication to restrict access including application and network-specific access requirements. Customer networks and systems are separated from QTS internal systems and other customer systems through the use of separated network segments. Additionally, two-factor authentication and use of a secure VPN is required for all remote access to customer networks and systems.

For customers with environments managed by QTS, customers can request secure connection to their systems through the setup of a VPN. The VPN solution protects the customer's user authentication information and the corresponding information transmitted over public networks. The customer environment is also segmented using Firewalls which restricts inbound and outbound traffic, multiple VLANs, and access control lists in order to restrict customer access to their own confidential information.

Threat and vulnerability management

QTS has a Threat and Vulnerability Management program to help identify potential threats and vulnerabilities against internal QTS systems and networks. QTS evaluates the risk, threats and vulnerabilities by defining a risk category, documenting the asset type, defining the risk, documenting the threat and vulnerability, determining the likelihood for the threat and/or vulnerability to occur and determining if the threat and/or vulnerability occurring caused a risk impact to QTS. QTS also documents compensating controls associated with the identified risks, threats and vulnerabilities, and ensures that identified areas have been concluded to an appropriate risk level.

As part of the Threat and Vulnerability Management program, QTS utilizes an intrusion detection systems to assist in minimizing the effect of a security incident through a malicious attack. When a security incident is identified during intrusion monitoring, a notification is sent to the OSC and a ticket is automatically opened in ServiceNow. The ticket is reviewed by the OSC support staff and assigned to the ISO and appropriate technical group for resolution. If a security Incident is identified by an employee or customer, the OSC is notified and relevant information is captured in a pre-defined standardized form. The security incident is then assigned to the appropriate individuals for research and resolution as necessary.

Antivirus software is used on QTS issued computers for protection against previously identified viruses.

System development and change management

QTS' Systems Development Life Cycle ("SDLC") defines a methodology that governs the design, acquisition, implementation, configuration, maintenance, modification, and management of infrastructure components. The SDLC governance helps to keep system additions or modifications consistent with security, availability, and confidentiality policies. To maintain a strong SDLC environment, QTS has defined the job descriptions specifying responsibilities and professional requirements for the roles that are responsible for the steps within the SDLC. Additionally, QTS evaluates its security, availability, and confidentiality tool requirements (e.g., utilities, software, hardware, etc.) on an ongoing basis. Any requests and determination for tool requirements arise from product development and implementation, security monitoring, and controls assessments performed by QTS.

A key part of the SDLC methodology is the Change Management process. Change Management is defined as the sequential steps and related activities necessary to successfully plan, approve, test, and authorize changes before implementation. The process encompasses internal changes to QTS services or supporting infrastructure (hardware, software, devices, and/or appliances), and is initiated when a change has the potential to impact the delivery of any internal or customer service. This process applies to critical (customer-impacting) applications, servers and databases. Changes are predominantly infrastructure related or the application of updates to vendor provided solutions where there is no real development required by QTS employees.

Submitting a change request

The requesting party must complete in its entirety the Change Request Submission Template found on the QTS portal. In addition, a Method of Procedure ("MOP") can be completed which further details the change methodology. Non-emergency changes are planned in advance of the work to be performed to allow for the Change Advisory Board ("CAB") approval and to provide customers with a minimum of seven days' notice prior to the commencement of changes potentially impacting customers. Once reviewed for completeness and accuracy by the CAB, the change is assigned a unique ticket number and added to the Request for Change ("RFC") agenda for discussion at the upcoming weekly CAB meeting. Refer to the above description for further specifics surrounding the CAB Committee. If the change management team does not receive a completed Request for Change (RFC) by close of business Friday for Tuesday CAB meetings or by close of business Tuesday for Thursday CAB meetings, the change request will not be added to the RFC agenda.

Approval process

The CAB meets on a weekly basis to discuss change requests on the RFC agenda. The submitting LOB requestor or Change Lead presents the change request to the CAB, responds to comments or concerns by the CAB, and subsequently asks for CAB approval. A formal CAB vote is taken, either approving or denying the change request for cause. If approved, the change request is placed on the Change Control Management Calendar, which is accessible to members of the organization. The CAB contains at least five QTS personnel that have the following title and authority to approve: Senior Manager, Director, VP, EVP, and/or Executive.

Customer notification

Once approval has been obtained from the CAB, OSC personnel develop and deliver a broadcast email to potentially impacted customers at least seven days prior to the maintenance window. The list of potentially impacted customers is documented, on the change request ticket. The automated-email tool is utilized in ServiceNow which includes an Information Technology Service Management system ("ITSM") that actively contacts potentially impacted customers.

Implementation of the change

QTS has a weekly rotating after-hours Change Manager role, comprised of middle management, to provide ownership for changes. The Change Manager, during his/her assigned week, is responsible for overseeing the adherence to policies and procedures throughout the change, communicating the initiation and completion of the change, and performing escalations should a problem occur during the change. Changes occurring during normal business hours are overseen by the manager corresponding to the group that is performing the change. Changes to critical applications, servers and databases are tested in the development environment where applicable and approved within the workflow ServiceNow prior to production implementation. Where it is not applicable to test the change before production implementation, the change manager has another change manager review the change within a peer review process. Changes are implemented into production by authorized personnel. If any changes fail, the CAB completes a post-implementation review as necessary during the weekly CAB call to identify if any changes failed. As mentioned before, changes are predominantly infrastructure related or the application of updates to vendor provided solutions where there is no real development required by QTS employees.

After the implementation of the change

After the change is complete, it is the responsibility of the Change Manager to email the members of the CAB indicating success. Should a change fail, a summary of the reasons for failure and subsequent outcomes are attached to the email. If physical changes to the infrastructure were made, it is the responsibility of the submitting LOB to provide the appropriate schematics and/or configuration documentation updates in a timely manner. Physical changes can include, but are not limited to, moving a cable, installing or removing a server, relocating a server, and running new cable.

Emergency changes

QTS' process for emergency changes follows the Change Management process described above, except they are initiated when a prompt change request must take place inside of the required seven days for approval allowing for proper planning of the change and customer communication.

Similar to non-emergency changes, the party requesting an emergency change must complete the Change Request Submission Template. The template is emailed to the Change Control Management Chair, a position within the Business Process Group ("BPG"), and must be approved by two LOB Senior Manager level (or higher) personnel prior to submission. This methodology validates that management has ownership and knowledge of the emergency change request and agrees with the risks associated with proceeding outside the standard Change Management process.

Once reviewed for completeness and accuracy, the change is assigned a unique ticket number in ServiceNow and assigned to an OSC personnel awaiting approval. In the event of a critical break-fix scenario, the on-site lead engineering personnel are empowered to affect immediate changes in order to restore service(s) or avoid service disruption(s). Other aspects of the Change Management process, in relation to emergency changes, apply as stated above and are performed as soon as possible.

System configuration reviews

On an annual basis, configurations on supporting infrastructure and software components are reviewed against the QTS defined configuration requirements, which are maintained by each applicable department, and current available software releases to determine if systems are consistent with security, availability and confidentiality policies. If any discrepancies are identified, research is performed to determine and document the rationale to perform remediation of the discrepancy. If necessary, the system is updated to the QTS defined configuration requirements by following the change management process described above.

Backup and storage management

QTS utilizes the Aptare tool to schedule data backups of critical QTS data center management systems. The Aptare tool is also used to monitor the backup for any errors that occur. On a daily basis, a report is generated for errors which are then automatically emailed to the OSC who will review the report and open an applicable ticket in ServiceNow to initiate the resolution of the identified errors.

QTS uses the Netbackup Vault tool as documented below to manage the backups that are saved on tape. On a daily basis Netbackup automatically sends a FTP file to QTS' third party vendor's Secure Sync portal that manages QTS' offsite backup storage. The Secure Sync portal indicates the files have been sent off-site and their applicable retention periods. The Data Center Operations ("DCO") team uses the Secure Sync portal to identify what backup tapes are to be pulled from the tape library and secured for off-site transportation. The DCO team also assists with the tapes being delivered back to the facility.

The Backup and Storage team provides customers an inventory of their backup tapes and their locations upon request. The Netbackup Vault systematically tracks the location of the backup tapes. Additionally, the Storage and Backup teams periodically perform inventories of backup tapes and tests the recoverability of the media.

Disaster recovery and business continuity program

The QTS Organizational Resilience Plan ("QTS ORP") includes well-defined and documented procedures, upon which the QTS staff is trained and able to respond and manage unforeseen events. QTS utilizes a step-by-step, standardized incident management process that ensures requirements relating to proper response, escalation, notification and resolution of a disruption of any type are met. The QTS ORP is integrated with QTS' physical and information security, and risk management systems. The QTS ORP adopts a process approach for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving the organization's resilience management system.

The disaster recovery plan is composed of a number of sections that document resources and procedures for recovering data center processing of applications should a disaster substantially disrupt operations. Each supported application or platform has a section containing specific recovery procedures. There are also sections that document the personnel that will be needed to perform the recovery tasks and an organizational structure for the recovery process.

The plan is updated as necessary and approved annually to reflect current hardware, software, procedures, applications, and staffing. Revisions are distributed to the disaster recovery team members at least twice a year following the disaster recovery tests.

Redundancy

One of the key components of emergency preparedness is to verify critical personnel and system redundancies, as indicated by the risk assessment, are in place for a facility's continuous operation during a crisis event. QTS has redundancies in place including QTS' UPS and generator power, network infrastructure, and hardware. Critical infrastructure, such as DNS and email servers, are duplicated across geographically diverse sites, and critical security log data is backed up and stored off site. To ensure vital service desk functions are performed during an emergency, QTS maintains a disaster recovery OSC separate from the main OSC. On-site backup facility staff undergo regular training and drills related to service desk and emergency procedures. The results of these drills are evaluated to identify opportunities for improvement.

Crisis and emergency response procedures

QTS has developed a set of policies and procedures governing crisis-major incident response which give guidance on the activities surrounding general emergency response, and empower the OSC to respond quickly and appropriately. These procedures govern the detection of service-impacting events, the processing of timely communications and escalations, the invocation of disaster recovery personnel, the method and mechanism of customer notifications and updates, the remote access to critical systems, and the notification of resolution through an After Action Report. QTS conducts regular company-wide training on these procedures to include regular testing that involves all lines of business. The results of the crisis and emergency response tests are scored and reviewed by management for continual process improvement considerations. These procedures are supplemented by site and event-specific emergency response procedures that are developed in response to the unique risks that specific facilities face. These procedures cover a variety of risks, including natural disasters such as earthquakes, pandemic flu, and terrorist attacks. These procedures are reviewed annually at minimum, and tests of emergency response are conducted and reviewed.

Relevant aspects of the control environment, risk assessment process, monitoring, and information and communication

QTS utilizes the 2013 Committee of Sponsoring Organizations Integrated of the Treadway Commission (COSO) Internal Control – Integrated Framework to develop and maintain an effective and efficient system of internal controls. The framework contains five components of Control Environment, Risk Assessment, Control Activities, Information & Communication, and Monitoring. The following descriptions provide an overview of these components within QTS:

Control environment

QTS' control environment sets the tone of the organization and influences the actions of QTS employees by providing accountability, principles and structure. The environment is comprised of QTS Core Values and governance activities performed by The Board of Directors ("Board"), Internal Audit, and Management Team.

QTS core values

QTS management has developed the QTS Core Values which are comprised of:

- Integrity, Character, Trust
- Action, Innovation, Accountability
- Team-Oriented
- Respect Our Customers
- Support of Family, Faith, and Community Volunteerism

These values are demonstrated to employees during on-boarding, through management's example, and communicated to employees periodically through "all hands meetings". An Employee Handbook detailing the Code of Ethics and defining ethical standards is also distributed and electronically certified by all employees. Other employee conduct items described in the Employee Handbook include:

- Conflicts of Interest
- Customer Relations
- Competition and Fair Dealing
- Confidentiality
- Protection and Use of QTS Records
- Violation of the Employee Handbook
- Disciplinary Actions

Updates to the Employee Handbook are communicated to employees in a company-wide message annually or more frequent as changes occur. QTS has established a third-party managed hotline for employees to anonymously voice any concerns. Complaints and notifications of misconduct or violations of any regulations received via the hotline or directly by senior management are communicated to the in-house General Counsel, Board members or the Chief People Officer.

Board of directors

The business and affairs of QTS are managed by QTS Realty Trust, Inc., with oversight from the Board of Quality Tech, LP. The Board is made up of individual members selected by the Nominating Committee. The Board meets quarterly, at a minimum, to discuss the business of QTS and meets more frequently if required to take action with respect to decisions as defined in the Bylaws. The Board sets the tone and direction for QTS and provides input and advice in the specialized areas represented at the Board level. Additionally, the Board oversees the Audit Committee, Compensation Committee, Nomination and Governance Committee, and any other committees established by the Board.

Audit committee

The Audit Committee is a standing committee of, and reports to, the Board. The Audit Committee oversees the accounting, financing, and compliance practices of QTS. QTS communicates with and reviews the activities and effectiveness of QTS' internal and external independent auditors. The committee confirms the independence of the external auditors ensuring compliance with the rules of the Securities Exchange Commission (SEC) and American Institute of Certified Public Accountants (AICPA). With the assistance of Management, the committee oversees the independent auditor's scope and planned approach on audits as they relate to financial reporting and compliance. The Audit Committee meets at least quarterly and receives reports from the Chief Financial Officer, Chief Accounting Officer, and the Chief Audit Executive.

Internal audit

The Internal Audit department is an independent and objective function with activities designed to add value and improve QTS' operations. Internal Audit helps QTS accomplish objectives by bringing a systematic and disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes. The Chief Audit Executive reports to the Audit Committee quarterly and notifies the committee of significant items related to internal controls and processes, audit findings, and other significant changes that have a potential impact to QTS. The Internal Audit department is based out of QTS' corporate headquarters in Overland Park, Kansas.

Management team

Management instills a philosophy that enables employees to share in the successes and ultimate growth of QTS. The management team is composed of a highly skilled and diverse group of employees who are ultimately responsible for the vision and direction of QTS. The management team regularly meets to discuss a wide range of topics and is responsible for establishing policy and addressing operational, financial, and social objectives of the organization. The organization strives to foster a working environment built on ethical standards which encourages communication and open forum discussions in a wide range of areas, ranging from technical issues on software development to ways to improve the internal corporate culture. Employees are routinely evaluated and given feedback from their managers regarding their professional skills and performance.

Risk assessment

QTS' risk assessment policy and procedures encompass QTS' entire organization and infrastructure. On an annual basis or when significant changes to the system occur, management performs a risk assessment on key areas including Business Continuity, Security, Finance, and Corporate IT. The risk assessment covers the following:

- Identification of potential threats and vulnerabilities that could impair the security, availability, confidentiality, and/or integrity of customer and QTS data (including relevant Protected Health Information);
- Assessment of the effect that environmental, regulatory, and technological changes have on the system's security, availability, confidentiality; and,
- Assessment of the risks associated with the identified threats.

Additionally, management performs a technical risk assessment of key technical service delivery components contained such as applications, devices, and servers which are included within the scope of this report to meet commitments to user entities. Management and Internal Audit communicate the risk assessment results to the Audit Committee. The Internal Audit plan is developed based on the risks identified during risk assessments.

Control activities

QTS has implemented policies and procedures to help verify that management directives are followed. Processes and controls exist to address risks in achieving the organization's stated objectives. Control activities operate throughout the organization at all levels and in all functions. Control activities relevant to the scope of this report are described further within "Information and Technology General Control System Operations" of Section III. Additionally, relevant control activities to address the AICPA criteria common to Trust Services Principles of Security, Availability and Confidentiality as well as specific criteria relevant to the Availability and Confidentiality Trust Services Principles are listed in Section IV of this report.

Information & communication

Management develops and maintains QTS policies and procedures, which are communicated to employees via the QTS document repository tool, during employee training, and within the employee handbook. QTS holds management meetings on a routine basis. The meetings include a series of reports from each of the managers identifying recent and forecasted key business activity and other ancillary issues.

Information and Communication activities relevant to the scope of this report are described further within "Services Control Descriptions" of this Section III. Additionally, relevant information and communication activities to address the AICPA criteria common to Trust Services Principles of Security, Availability and Confidentiality as well as specific criteria relevant to the Availability and Confidentiality Trust Services Principles are listed in Section IV of this report.

Monitoring

QTS has a dedicated compliance function which continuously monitors controls and takes appropriate actions as necessary by updating controls, policies and procedures accordingly. Internal controls are closely observed to verify that they are operating as designed. The organization's monitoring policy calls for reviewing aspects of the enterprise-wide network on a periodic basis, coupled with discussions as needed on additional controls for areas such as employee issues, business continuity management, building security, network security, and other areas or subject matters deemed vital to QTS' data center activities. Management monitors controls through a combination of periodic evaluations and ongoing activities. Periodic evaluations include reviews performed by internal and external auditors as well as Line of Business ("LOB") management to identify strengths and weaknesses in internal controls.

Ongoing activities include recurring functions, such as communications with external parties (customers and vendors), periodic scans for unauthorized WIFI access points, and evaluations of security events, which are performed by personnel as part of their daily activities and provide information regarding the effectiveness of internal controls. Controls found to be weak or ineffective are reported and appropriate corrective actions are initiated.

Section IV - Trust services principles, criteria, related controls and KPMG LLP’s tests of controls and results of tests

Principles, criteria and QTS Realty, Inc'.s related controls and KPMG LLP's tests of controls and results of tests

Principles:

Security – The system is protected against unauthorized access, use, or modification.

Availability – The system is available for operation and use as committed or agreed.

Confidentiality – Information designated as confidential is protected as committed or agreed.

KPMG Tests of Operating Effectiveness

When using information produced by QTS, which includes, but is not limited to, management's reports used in the performance of controls and reports generated to facilitate testing of control populations, KPMG evaluated whether the information was sufficiently reliable for our purposes, including, as necessary, obtaining evidence about the completeness and accuracy of the information and evaluating whether the information was sufficiently precise and detailed for our purposes.

Criteria CC1.0	**Common Criteria Related to Organization and Management: The criteria relevant to how the organization is structured and the processes the organization has implemented to manage and support people within its operating units. This includes criteria addressing accountability, integrity, ethical values and qualifications of personnel, and the environment in which they function.**

CC1.1	The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance and monitoring of the system enabling it to meet its commitments and system requirements as they relate to security, availability and confidentiality.	
QTS Description of control	**KPMG's Test of controls**	**KPMG Results of tests**
CC1.1.1 – As needed, QTS Senior Management reviews, and adjusts as necessary the entity's organizational charts that set forth the lines of reporting and responsibility areas to meet changing entity commitments and requirements.	Inspected QTS organization charts to determine whether reporting and responsibility areas were established, reviewed periodically by senior management, and have been updated as necessary. Inspected a selection of department's organizational charts as relates to Security, Availability and Confidentiality to determine whether there are individuals assigned with appropriate reporting lines, authorities, and responsibilities to support the system.	No exceptions noted.
CC1.1.2 – QTS People Services maintains a description of the organization structure, processes, and organizational roles and responsibilities on the QTS intranet to identify the parties responsible for the design, development, implementation, and operation of systems.	Inspected QTS's intranet to determine whether QTS maintains a description of the organization structure, processes, and organizational roles and responsibilities to identify the parties responsible for the design, development, implementation, and operation of systems.	No exceptions noted.

CC1.1	The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance and monitoring of the system enabling it to meet its commitments and system requirements as they relate to security, availability and confidentiality.

QTS Description of control	KPMG’s Test of controls	KPMG Results of tests
CC1.1.3 – As needed, the People Services Department posts, reviews, and updates written job descriptions located on the entity's intranet specifying the roles, responsibilities, professional, and academic requirements for positions impacting the security, availability and/or confidentiality of QTS services including those which are responsible for the design, development, implementation, and operation of systems.	Inspected a sample of key job descriptions to determine whether QTS has written job descriptions specifying the responsibilities and academic and professional requirements for key job positions, including those which are responsible for the design, development, implementation, and operation of systems affecting security, availability and/or confidentiality, and that policies have been updated as necessary.	No exceptions noted.

Complementary User Entity Controls:

Not Applicable

Criteria CC1.2	Responsibility and accountability for designing, developing, implementing, operating, maintaining, monitoring, and approving the entity's system controls and other risk mitigation strategies are assigned to individuals within the entity with authority to ensure policies and other system requirements are effectively promulgated and implemented to meet the entity's commitments and system requirements as they relate to security, availability and confidentiality.

QTS Description of control	KPMG's Test of controls	KPMG Results of tests
CC1.2.1 – The QTS Corporate Policy Committee is responsible and accountable for designing, developing, implementing, operating, maintaining, monitoring, and approving the entity's system controls and other risk mitigation strategies. The Committee sets the QTS policy management methodology for the QTS policy set so that QTS policy meets business requirements. The Committee operates and sets methodology per the Corporate Policy Committee Charter.	Inspected the QTS policy management methodology for the QTS policy set to determine whether it covers the development and approval of QTS security, availability and confidentiality policies. Inspected the QTS policy management methodology to determine if the Corporate Policy Committee oversees adherence to the QTS policy management methodology per the QTS Corporate Policy Committee Charter, and policy updates were approved by the QTS Corporate Policy Committee.	No exceptions noted.

Criteria CC1.2	Responsibility and accountability for designing, developing, implementing, operating, maintaining, monitoring, and approving the entity's system controls and other risk mitigation strategies are assigned to individuals within the entity with authority to ensure policies and other system requirements are effectively promulgated and implemented to meet the entity's commitments and system requirements as they relate to security, availability and confidentiality.

QTS Description of control	KPMG's Test of controls	KPMG Results of tests
CC1.2.2 – The QTS Corporate Policy Committee oversees adherence to the QTS policy management methodology for the QTS policy set so that QTS policy is in compliance with the established methodology. The Committee reviews to determine whether policies identify owners and scope, are updated as required, and are reviewed annually at a minimum prior to publishing to the QTS policy set per the Document Governance specification.	Inspected QTS policies, procedures and specifications to determine whether the documents have been established that: a. Address the security, availability, and confidentiality of its services b. Identify policy owners and scope c. Have been reviewed annually and updated as necessary and, d. Any new/significantly changed policies have been communicated to all users and available on the company's intranet.	No exceptions noted.
Complementary User Entity Controls: Not Applicable		

Criteria CC1.3	The entity has established procedures to evaluate the competency of personnel responsible for designing, developing, implementing, operating, maintaining and monitoring the system affecting security, availability and confidentiality and provides resources necessary for personnel to fulfill their responsibilities.

QTS Description of control	KPMG’s Test of controls	KPMG Results of tests
CC1.3.1 – Annually, the QTS People Services Department monitors the completion of employees performance evaluations located in the HR system so that employees maintained qualifications to fulfill their daily responsibilities.	Inspected supporting documentation for a sample of employees to determine whether performance evaluations were completed yearly and whether management tracks employee participation to confirm all employees maintain qualifications to fulfill their daily responsibilities.	No exceptions noted.
CC1.3.2 – The QTS Training Department requires all employees complete the security awareness training through the Learning Management System upon hire and annually thereafter to so that employees acknowledge they have read and accept the entity's security, availability, and confidentiality policies and understand their responsibility and accountability for those policies.	Inspected the security awareness training documentation to determine whether QTS provides annual security awareness training to employees which informs employees about the company's security, availability and confidentiality commitments and the process for identifying and reporting possible system availability issues, security breaches, confidentiality breaches, and other incidents. Inspected a sample of new hire and existing employee acknowledgements of the annual security awareness training to determine whether management tracks employee participation to confirm all employees’ complete training.	No exceptions noted.

Criteria CC1.3	The entity has established procedures to evaluate the competency of personnel responsible for designing, developing, implementing, operating, maintaining and monitoring the system affecting security, availability and confidentiality and provides resources necessary for personnel to fulfill their responsibilities.

QTS Description of control	KPMG's Test of controls	KPMG Results of tests
CC1.3.3 – The QTS Training Department identifies requirements via needs assessments, develops training materials, and delivers employee security, availability, confidentiality training using the Learning Management System to develop and enhance employee knowledge of QTS processes.	Inspected a sample of training courses included in QTS' training curriculum to determine whether the QTS training department identified requirements, developed training materials and delivered employee training to meet availability, security, and confidentiality requirements.	No exceptions noted.
CC1.3.4 – Quarterly, QTS Facilities Department requires all personnel related to Data Center Operations, Critical Environmental, Site Services Technicians and electrical/mechanical positions to successfully complete safety training courses available in TPC Online to maintain knowledge of federal and State regulations.	Inspected supporting documentation for a sample of Data Center Operations, Critical Environmental, Site Services Technicians and Electrical/Mechanical employees to determine whether the QTS Facilities Department required safety training to be completed quarterly, and that Federal and State regulations were included within the trainings.	No exceptions noted.

Criteria CC1.3	The entity has established procedures to evaluate the competency of personnel responsible for designing, developing, implementing, operating, maintaining and monitoring the system affecting security, availability and confidentiality and provides resources necessary for personnel to fulfill their responsibilities.

QTS Description of control	KPMG’s Test of controls	KPMG Results of tests
CC1.3.5 – Bi-weekly, the QTS Technical Advisory Committee (TAC) meets when there are requests to review new software implementations arising from product development, security monitoring, or controls assessments to approve, defer, or reject requests. The process is performed per the QTS Technical Advisory Committee charter.	Inspected a sample of minutes from the bi-weekly QTS Technical Advisory Committee (TAC) meetings to determine whether management reviewed, approved, deferred or rejected new software implementations arising from product development, security monitoring, or controls assessments.	No exceptions noted.

Complementary User Entity Controls:

Not Applicable

Criteria CC1.4	The entity has established workforce conduct standards, implemented workforce candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and requirements as they relate to security, availability and confidentiality.

QTS Description of control	KPMG's Test of controls	KPMG Results of tests
CC1.4.1 – QTS People Services requires new employees, upon hire, to acknowledge and accept that they will follow QTS employment policies and employee conduct requirements defined in the Employee Handbook to so that employees are informed of these requirements. Employee violations of the Employee Handbook are managed by People Services and Legal as required. The Employee Handbook is available to all employees on the QTS intranet and employee acceptance is recorded through electronic signature.	Inspected the Employee Handbook to determine if it covers employment policies and employment conduct, if violations are handled by People Services and/or Legal, and if the Employee Handbook is available to all employees on the QTS intranet. Inspected supporting documentation for a sample of new employees to determine whether new employees acknowledged and electronically accepted review of the Employee Handbook. Inspected supporting documentation for a sample of employee violations of the Employee Handbook to determine whether employee violations are managed by People Services and Legal as required.	No exceptions noted.
CC1.4.2 – QTS People Services performs a background check consisting of criminal convictions, drug screening, and employment verification for all prospective employees within ten (10) calendar days of employment to support QTS' commitments by employing qualified personnel. Background checks are performed per the Background Screening specification.	Inspected the Background Screening specification and supporting documentation for a sample of new employees to determine whether criminal background checks were evaluated within 10 days of employment and if the background check consisted of the following checks; criminal convictions state and federal (prior seven years), drug screening, employment verification (prior seven years).	No exceptions noted.

Criteria CC1.4	The entity has established workforce conduct standards, implemented workforce candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and requirements as they relate to security, availability and confidentiality.

QTS Description of control	KPMG's Test of controls	KPMG Results of tests
CC1.4.3 – QTS People Services requires prospective employees to electronically sign a non-disclosure agreement (NDA) and/or confidentiality agreements (CA) within ten (10) calendar days of employment so that QTS data is kept confidential.	Inspected non-disclosure agreements and/or confidentiality agreements for a sample of new employees to determine whether agreements were signed within 10 days of employment.	Exceptions noted. KPMG determined that 1 user out of the selected sample of new employees did not sign their non-disclosure and/or confidentiality agreement within 10 days of employment. Please see section V for management's response to the exception.

Complementary User Entity Controls:

Not Applicable

Criteria CC2.0	**Common Criteria Related to Communications: The criteria relevant to how the organization communicates its policies, processes, procedures, commitments, and requirements to authorized users and other parties of the system and the obligations of those parties and users to the effective operation of the system**

Criteria CC2.1	Information regarding the design and operation of the system and its boundaries has been prepared and communicated to authorized internal and external users of the system to permit users to understand their role in the system and the results of system operation.	
QTS Description of control	**KPMG's Test of controls**	**KPMG Results of tests**
CC2.1.1 – As needed, the People Services Department posts, reviews, and updates written job descriptions located on the entity's intranet specifying the roles, responsibilities, professional, and academic requirements for positions impacting the security, availability and/or confidentiality of QTS services.	Inspected a sample of key job descriptions to determine whether QTS has written job descriptions specifying the responsibilities and academic and professional requirements for key job positions, including those which are responsible for the design, development, implementation, and operation of systems affecting security, availability and/or confidentiality, and that policies have been updated as necessary.	No exceptions noted.
CC2.1.2 – The QTS Product Department posts all product descriptions, sales materials, administrative guides, the acceptable use policy, and standards of procedures in SharePoint and the QTS public website in order to define the roles and responsibilities of employees and external users.	Inspected QTS's public website and SharePoint to determine whether QTS has posted product descriptions, sales materials, administrative guides, the acceptable use policy, and standards of procedures for review by QTS employees and external users.	No exceptions noted.
Complementary user entity controls: Not Applicable		

Criteria CC2.2	The entity's security, availability and confidentiality commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal system users to enable them to carry out their responsibilities.

QTS Description of control	KPMG's Test of controls	KPMG Results of tests
CC2.2.1 – QTS communicates to customers' roles and responsibilities and security, availability, and confidentiality commitments within the Data Center handbook located on the Customer Portal and the executed customer agreements. The Customer Portal lists the customer's responsibilities and process to report operational failures, incidents, problems, concerns and complaints.	Inspected QTS' customer portal to determine whether the data center handbook is available and customers' responsibilities, which include responsibility for reporting operational failures, incidents, problems, concerns and complaints, and the process for doing so, are also described in the customer portal. Inspected a sample of Data center handbooks and executed customer agreements to determine whether the entity's security, availability, and confidentiality commitments, roles and responsibilities were included.	No exceptions noted.
CC2.2.2 – QTS has defined charters, policies, procedures and specification documents that communicate QTS' commitments and associated system requirements to internal users to enable them carry out their responsibilities.	Inspected QTS policies, procedures and specifications to determine whether the documents have been established to communicate QTS' commitments and associated system requirements to internal users to enable them carry out their responsibilities.	No exceptions noted.

Criteria CC2.2	The entity's security, availability and confidentiality commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal system users to enable them to carry out their responsibilities.

QTS Description of control	KPMG's Test of controls	KPMG Results of tests
CC2.2.3 – The QTS Training Department requires all employees complete the security awareness training through the Learning Management System upon hire and annually thereafter so that employees acknowledge they have read and accept the entity's security, availability, and confidentiality policies and understand their responsibility and accountability for those policies.	Inspected the security awareness training documentation to determine whether QTS provides annual security awareness training to employees which informs employees about the company's security, availability and confidentiality commitments and the process for identifying and reporting possible system availability issues, security breaches, confidentiality breaches, and other incidents. Inspected a sample of new hire and existing employee acknowledgements of the annual security awareness training to determine whether management tracks employee participation to confirm all employees' complete training.	No exceptions noted.
CC2.2.4 – The QTS Training Department identifies requirements via needs assessments, develops training materials, and delivers employee security, availability, confidentiality trainings using the Learning Management System to develop and enhance employee knowledge of QTS processes.	Inspected a sample of training courses included in QTS' training curriculum to determine whether the QTS training department identified requirements, developed training materials and delivered employee training to meet availability, security, and confidentiality requirements.	No exceptions noted.
Complementary User Entity Controls: Not Applicable		

Criteria CC2.3	The responsibilities of internal and external users and others whose roles affect system operation are communicated to those parties.

QTS Description of control	KPMG's Test of controls	KPMG Results of tests
CC2.3.1 – QTS has defined charters, policies, procedures and specification documents that communicate the responsibilities of internal users whose roles affect system operation.	Inspected QTS policies, procedures and specifications to determine whether the documents have been established to communicate the responsibilities of internal users whose roles affect system operation.	No exceptions noted.
CC2.3.2 – The QTS Training Department requires all employees complete the security awareness training through the Learning Management System upon hire and annually thereafter so that employees acknowledge they have read and accept the entity's security, availability, and confidentiality policies and understand their responsibility and accountability for those policies.	Inspected the security awareness training documentation to determine whether QTS provides annual security awareness training to employees which informs employees about the company's security, availability and confidentiality commitments and the process for identifying and reporting possible system availability issues, security breaches, confidentiality breaches, and other incidents. Inspected a sample of new hire and existing employee acknowledgements of the annual security awareness training to determine whether management tracks employee participation to confirm all employees' complete training.	No exceptions noted.
CC2.3.3 – The QTS Training Department identifies requirements via needs assessments, develops training materials, and delivers employee security, availability, confidentiality trainings using the Learning Management System to develop and enhance employee knowledge of QTS processes.	Inspected a sample of training courses included in QTS' training curriculum to determine whether the QTS training department identified requirements, developed training materials and delivered employee training to meet availability, security, and confidentiality requirements.	No exceptions noted.

<table>
<tr><td>Criteria CC2.3</td><td colspan="2">The responsibilities of internal and external users and others whose roles affect system operation are communicated to those parties.</td></tr>
<tr><th>QTS Description of control</th><th>KPMG’s Test of controls</th><th>KPMG Results of tests</th></tr>
<tr><td>CC2.3.4 –
QTS People Services maintains a description of the organization structure, processes, and organizational roles and responsibilities on the QTS intranet to identify the parties responsible, accountable, consented, and informed of changes in design and operation of key system components.</td><td>Inspected QTS’s intranet to determine whether QTS maintains a description of the organization structure, processes, and organizational roles and responsibilities to identify the parties responsible, accountable, consented, and informed of changes in design and operation of key system components.</td><td>No exceptions noted.</td></tr>
<tr><td>CC2.3.5 –
QTS communicates to customers’ roles and responsibilities and security, availability, and confidentiality commitments within the Data Center handbook located on the Customer Portal. The Customer Portal lists the customer's responsibilities and process to report operational failures, incidents, problems, concerns and complaints.</td><td>Inspected QTS' customer portal to determine whether the data center handbook is available and customers' responsibilities, which include responsibility for reporting operational failures, incidents, problems, concerns and complaints, and the process for doing so, are also described in the customer portal.
Inspected a sample of Data center handbooks to determine whether the entity’s security, availability, and confidentiality commitments, roles and responsibilities were included.</td><td>No exceptions noted.</td></tr>
<tr><td colspan="3">Complementary User Entity Controls:
Not Applicable</td></tr>
</table>

Criteria CC2.4	Information necessary for designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the security, availability, and confidentiality of the system, is provided to personnel to carry out their responsibilities.

QTS Description of control	KPMG's Test of controls	KPMG Results of tests
CC2.4.1 – QTS has defined charters, policies, procedures and specification documents that provide internal system personnel the information necessary to carry out those responsibilities.	Inspected QTS policies, procedures and specifications to determine whether the documents have been established to provide internal system personnel the information necessary to carry out those responsibilities.	No exceptions noted.
CC2.4.2 – QTS People Services maintains a description of the organization structure, processes, and organizational roles and responsibilities on the QTS intranet to identify the parties responsible, accountable, consented, and informed of changes in design and operation of key system components.	Inspected QTS's intranet to determine whether QTS maintains a description of the organization structure, processes, and organizational roles and responsibilities to identify the parties responsible, accountable, consented, and informed of changes in design and operation of key system components.	No exceptions noted.

Criteria CC2.4	Information necessary for designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the security, availability, and confidentiality of the system, is provided to personnel to carry out their responsibilities.	
QTS Description of control	**KPMG's Test of controls**	**KPMG Results of tests**
CC2.4.3 – The Data Center Infrastructure Management (DCIM) Department monitors data center processes such as cooling and power to determine compliance with service level commitments and agreements 24x7x365. Alerts are generated by the Building Management System (BMS) and Electrical Power Management System (EPMS) and routed to appropriate parties for resolution per standard procedures in the event that processes are not in compliance.	Inspected Building Management System (BMS) and Electrical Power Management System (EPMS) monitoring configurations and a sample of real-time alerts/notifications that impact security/confidentiality, cooling, power, and uptime to determine whether the DCIM Department monitors and receives alerts 24x7x365 regarding the operations of the key systems in compliance with the service level commitments and agreements, system monitoring results are communicated to applicable personnel and customers, and actions are taken when service level commitments and agreements are not met.	No exceptions noted.
CC2.4.4 – QTS communicates to customers' roles and responsibilities and security, availability, and confidentiality commitments within the Data Center handbook located on the Customer Portal. The Customer Portal lists the customer's responsibilities and process to report operational failures, incidents, problems, concerns and complaints.	Inspected QTS' customer portal to determine whether the data center handbook is available and customers' responsibilities, which include responsibility for reporting operational failures, incidents, problems, concerns and complaints, and the process for doing so, are also described in the customer portal. Inspected a sample of Data center handbooks to determine whether the entity's security, availability, and confidentiality commitments, roles and responsibilities were included.	No exceptions noted.
Complementary User Entity Controls: Not Applicable		

Criteria CC2.5	Internal and external system users have been provided with information on how to report security, availability and confidentiality failures, incidents, concerns, and other complaints to appropriate personnel.

QTS Description of control	KPMG's Test of controls	KPMG Results of tests
CC2.5.1 – The Information Security Department has documented procedures available to internal users for the identification, notification and escalation of incidents via ServiceNow to determine that breaches, complaints and incidents are handled and communicated to the relevant internal and external parties.	Inspected system availability, breach, and complaint procedures to determine whether QTS has documented procedures for the identification, notification and escalation of possible system availability issues, security breaches, confidentiality breaches, complaints and other incidents.	No exceptions noted.
CC2.5.2 – The QTS Customer Portal lists the process to report security, confidentiality and operational availability failures, incidents, problems, concerns and complaints in the customer portal.	Inspected QTS' customer portal to determine whether customers' responsibilities, which include responsibility for reporting security, confidentiality, and availability operational failures, incidents, problems, concerns and complaints, and the process for doing so, are described in the customer portal.	No exceptions noted.
Complementary User Entity Controls: Not Applicable		

Criteria CC2.6	System changes that affect internal and external users' responsibilities or the entity's commitments and requirements relevant to security, availability, and confidentiality are communicated to those users in a timely manner.

QTS Description of control	KPMG’s Test of controls	KPMG Results of tests
CC2.6.1 – The QTS policy set is reviewed annually at a minimum prior to publishing to determine that changes or updates to owners and scope are appropriately captured.	Inspected QTS policies, procedures and specifications to determine whether the QTS policy set has been reviewed annually at a minimum prior to publishing to determine that changes or updates to owners and scope are appropriately captured.	No exceptions noted.
CC2.6.2 – The QTS Change Team notifies customers of potentially customer-impacting changes through ServiceNow seven days before maintenance is performed.	Inspected supporting documentation for a sample of customer-impacting changes to determine whether maintenance changes are communicated to impacted customers prior to implementation to production.	No exceptions noted.
Complementary User Entity Controls: Not Applicable		

Criteria CC3.0	**Common Criteria Related to Risk Management and Design and Implementation of Controls: The criteria relevant to how the entity (I) identifies potential risks that would affect the entity's ability to achieve its objectives, (ii) analyzes those risks, (iii) develops responses to those risks including the design and implementation of controls and other risk mitigating actions, and (iv) conducts ongoing monitoring of risks and the risk management process.**

Criteria CC3.1	The entity (1) identifies potential threats that would impair system security, availability, and confidentiality commitments and system requirements, (2) analyzes the significance of risks associated with the identified threats, and (3) determines mitigation strategies for those risks (including implementation of controls, assessment and monitoring of vendors and other third parties providing goods or services, as well as their activities, and other mitigation strategies), (4) identifies and assesses changes (for example, environmental, regulatory, and technological changes and results of the assessment and monitoring of controls) that could significantly affect the system of internal control, and (5) reassesses, and revises, as necessary, risk assessments and mitigation strategies based on the identified changes.

QTS Description of control	KPMG's Test of controls	KPMG Results of tests
CC3.1.1 – Annually, the Information Security Department performs a comprehensive vulnerability scan to identify potential risks to system security and confidentiality. Risks are reviewed and remediation plans are developed, reviewed by management, and mitigation completed.	Inspected the results of the annual comprehensive vulnerability scans to determine whether: a. Scans and testing are performed annually to identify potential risks to system security and confidentiality; b. Identified risks are reviewed and evaluated against the defined QTS security and confidentiality policies, service level agreements, and other QTS obligations; and; c. The assessment results and remediation plans are reviewed, approved, and monitored to determine completion of mitigation by Line of Business Owners and the ISO team.	No exceptions noted.
CC3.1.2 – Annually, the Information Security Department performs a technical risk assessment of key technical components in the QTS service delivery software and infrastructure to detect and remediate risks as necessary.	Inspected supporting documentation to determine whether QTS performs an annual technical risk assessment of key technical components which is reviewed by appropriate members of management and that risk mitigation actions are taken as necessary.	No exceptions noted.

Criteria CC3.1	The entity (1) identifies potential threats that would impair system security, availability, and confidentiality commitments and system requirements, (2) analyzes the significance of risks associated with the identified threats, and (3) determines mitigation strategies for those risks (including implementation of controls, assessment and monitoring of vendors and other third parties providing goods or services, as well as their activities, and other mitigation strategies), (4) identifies and assesses changes (for example, environmental, regulatory, and technological changes and results of the assessment and monitoring of controls) that could significantly affect the system of internal control, and (5) reassesses, and revises, as necessary, risk assessments and mitigation strategies based on the identified changes.

QTS Description of control	KPMG's Test of controls	KPMG Results of tests
CC3.1.3– Annually, the Internal Audit Department initiates a company-wide risk assessment, completed by relevant line of business management, to identify key risks that could affect the security, availability, or confidentiality of QTS services in areas such as business continuity, security and corporate IT.	Inspected the annual risk assessment, to determine whether QTS management performs a company-wide risk assessment to: a. Identify potential threats and vulnerabilities that could impair the security, availability, confidentiality, and/or integrity of customer and QTS data, b. Assess the effect that environmental, regulatory, and technological changes have on the system security, availability and confidentiality, and c. Assess the risks associated with the identified threats.	No exceptions noted.

Criteria CC3.1	The entity (1) identifies potential threats that would impair system security, availability, and confidentiality commitments and system requirements, (2) analyzes the significance of risks associated with the identified threats, and (3) determines mitigation strategies for those risks (including implementation of controls, assessment and monitoring of vendors and other third parties providing goods or services, as well as their activities, and other mitigation strategies), (4) identifies and assesses changes (for example, environmental, regulatory, and technological changes and results of the assessment and monitoring of controls) that could significantly affect the system of internal control, and (5) reassesses, and revises, as necessary, risk assessments and mitigation strategies based on the identified changes.

QTS Description of control	KPMG's Test of controls	KPMG Results of tests
CC3.1.4– Bi-weekly, The Compliance Department leads a meeting with the Information Security Department to monitor and reassess the current technology environment at QTS for the suitability of design and operational effectiveness of control activities and takes actions as appropriate to revise risk assessments and mitigation strategies based on identified changes. A summary of points discussed and action items are recorded in meeting minutes retained in SharePoint.	Inspected a sample of minutes from the bi-weekly Compliance Department and Information Security Department meetings to determine whether management monitors and assess the current technology environment at QTS for the suitability of design and operational effectiveness of control activities, discussion points and action items are recorded in the meeting minutes, and management takes actions as appropriate to revise risk assessments and mitigation strategies based on identified changes.	No exceptions noted.

Criteria CC3.1	The entity (1) identifies potential threats that would impair system security, availability, and confidentiality commitments and system requirements, (2) analyzes the significance of risks associated with the identified threats, and (3) determines mitigation strategies for those risks (including implementation of controls, assessment and monitoring of vendors and other third parties providing goods or services, as well as their activities, and other mitigation strategies), (4) identifies and assesses changes (for example, environmental, regulatory, and technological changes and results of the assessment and monitoring of controls) that could significantly affect the system of internal control, and (5) reassesses, and revises, as necessary, risk assessments and mitigation strategies based on the identified changes.

QTS Description of control	KPMG's Test of controls	KPMG Results of tests
CC3.1.5- The Compliance Department monitors regulatory changes to confirm the suitability of controls to meet current regulatory requirements and takes actions as appropriate. Monitoring is achieved through reviews of standards, updates to the QTS regulatory library in Keylight, and continuing professional education of Compliance personnel.	Inspected the QTS Compliance Charter, Compliance Division Organization Chart and the continuing professional education of Compliance personnel to determine whether QTS has a dedicated compliance function in place which continuously monitors controls and assesses changes to the environment that may impact controls. Inspected the QTS Keylight regulatory library to determine whether management assesses changes to the environment that may impact controls, takes appropriate actions from the continuous monitoring process and updates controls, policies and procedures accordingly.	No exceptions noted.
CC3.1.6- Annually, the Business Continuity Department and line of business owners' review, update, and approve QTS Business Continuity procedures to determine that accurate processes are in place to identify environmental changes and to meet defined availability, security, and contractual requirements.	Inspected QTS Business Continuity Procedures to determine if they are reviewed annually by the Business Continuity Department and line of business owners, and that processes are in place to identify environmental changes and to meet defined availability, security, and contractual requirements.	No exceptions noted.
Complementary User Entity Controls: Not Applicable		

Criteria CC3.2	The entity designs, develops, implements and operates controls, including policies and procedures, to implement its risk mitigation strategy; reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities; and updates the controls, as necessary.

QTS Description of control	KPMG's Test of controls	KPMG Results of tests
CC3.2.1 – QTS has defined charters, policies, procedures and specification documents to implement its risk mitigation strategy.	Inspected QTS policies, procedures and specifications to determine whether the documents have established its risk mitigation strategy.	No exceptions noted.
CC3.2.2 – Annually, the Information Security Department performs a comprehensive vulnerability scan to identify potential risks to system security and confidentiality. Risks are reviewed and remediation plans are developed, reviewed by management, and mitigation completed.	Inspected the results of the annual comprehensive vulnerability scans to determine whether: a. Scans and testing are performed annually to identify potential risks to system security and confidentiality; b. Identified risks are reviewed and evaluated against the defined QTS security and confidentiality policies, service level agreements, and other QTS obligations; and; c. The assessment results and remediation plans are reviewed, approved, and monitored to determine completion of mitigation by Line of Business Owners and the ISO team.	No exceptions noted.
CC3.2.3- Bi-weekly, The Compliance Department leads a meeting with the Information Security Department to monitor and assess the current technology environment at QTS for the suitability of design and operational effectiveness of control activities and takes actions as appropriate. A summary of points discussed and action items are recorded in meeting minutes retained in SharePoint.	Inspected a sample of minutes from the bi-weekly Compliance Department and Information Security Department meetings to determine whether management monitors and assess the current technology environment at QTS for the suitability of design and operational effectiveness of control activities, discussion points and action items are recorded in the meeting minutes, and management takes actions as appropriate.	No exceptions noted.

Criteria CC3.2	The entity designs, develops, implements and operates controls, including policies and procedures, to implement its risk mitigation strategy; reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities; and updates the controls, as necessary.

QTS Description of control	KPMG's Test of controls	KPMG Results of tests
CC3.2.4- The Compliance Department monitors regulatory changes to confirm the suitability of controls to meet current regulatory requirements and takes actions as appropriate. Monitoring is achieved through reviews of standards, updates to the QTS regulatory library in Keylight, and continuing professional education of Compliance personnel.	Inspected the QTS Compliance Charter, Compliance Division Organization Chart and the continuing professional education of Compliance personnel to determine whether QTS has a dedicated compliance function in place which continuously monitors controls and assesses changes to the environment that may impact controls. Inspected the QTS Keylight regulatory library to determine whether management reviews and assesses changes to the environment that may impact controls, takes appropriate actions from the continuous monitoring process and updates controls, policies and procedures accordingly.	No exceptions noted.

Complementary User Entity Controls:

Not Applicable

Criteria CC4.0	**Common Criteria Related to Monitoring of Controls: The criteria relevant to how the entity monitors the system, including the suitability, and design and operating effectiveness of the controls, and takes action to address deficiencies identified.**

Criteria CC4.1	The design and operating effectiveness of controls are periodically evaluated against the entity's commitments and system requirements as they relate to security, availability, and confidentiality and corrections and other necessary actions relating to identified deficiencies are taken in a timely manner.

QTS Description of control	KPMG's Test of controls	KPMG Results of tests
CC4.1.1 – Bi-weekly, The Compliance Department leads a meeting with the Information Security Department to monitor and assess the current technology environment at QTS for the suitability of design and operational effectiveness of control activities and takes actions as appropriate. A summary of points discussed and action items are recorded in meeting minutes retained in SharePoint.	Inspected a sample of minutes from the bi-weekly Compliance Department and Information Security Department meetings to determine whether management monitors and assess the current technology environment at QTS for the suitability of design and operational effectiveness of control activities, discussion points and action items are recorded in the meeting minutes, and management takes actions as appropriate.	No exceptions noted.
CC4.1.2 – The QTS Operations Department monitors the availability and performance of QTS service delivery and customer networks and systems 24x7x365 using the CA Unified Infrastructure Management monitoring tool which sends automated notifications to customers and/or QTS for critical events outside an acceptable range.	Inspected a sample of CA Unified Infrastructure Management customer and QTS automated alerts to determine whether alerts are generated when critical events or potential system or network disruption is detected. Inspected corresponding tickets to determine whether a ticket is generated, as appropriate, and routed to appropriate parties for resolution.	No exceptions noted.

Criteria CC4.1	The design and operating effectiveness of controls are periodically evaluated against the entity's commitments and system requirements as they relate to security, availability, and confidentiality and corrections and other necessary actions relating to identified deficiencies are taken in a timely manner.

QTS Description of control	KPMG's Test of controls	KPMG Results of tests
Complementary User Entity Controls: a. The user entity should review automated notifications that are generated and provided for certain events as specified by the user entity and notify QTS where further action is needed.		

Criteria CC5.0	**Common Criteria Related to Logical and Physical Access Controls: the criteria relevant to how the organization restricts logical and physical access to the system, provides and removes that access, and prevents unauthorized access to meet the criteria for the principle(s) addressed in the engagement.**

Criteria CC5.1	Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality. (Note: Mobile systems are N/A)

QTS Description of control	KPMG's Test of controls	KPMG Results of tests
CC5.1.1 – QTS Operations implements individual user network and application login credentials stored in the QTS Active Directory for the identification, authentication, and accountability of users' system access.	Inspected a sample of in-scope network, and application user accounts to determine whether the user IDs were assigned to individuals for ownership and accountability.	No exceptions noted.
CC5.1.2 – Network password parameters and account logon configurations covering password length, complexity, expiration, account lockout, and session timeout are implemented per QTS password specifications.	Inspected the network password configuration settings for the Jump, Compliance and Dulles domains to determine whether logon configurations are implemented covering password length, complexity, expiration, account lockout, and session timeout per the QTS password specification.	No exceptions noted.

Criteria CC5.1	Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality. (Note: Mobile systems are N/A)

QTS Description of control	KPMG's Test of controls	KPMG Results of tests
CC5.1.3 – The QTS Network Operations Department restricts traffic to authorized inbound and outbound traffic through the use of firewalls to protect networks in accordance with QTS firewall configuration standards. Firewall configuration standards are set to appropriately restrict unauthorized user access.	Inspected firewall configurations to determine whether QTS has firewalls in place to restrict inbound and outbound traffic or unauthorized user access, and that settings are in conformance with QTS Firewall configuration standards.	No exceptions noted.
CC5.1.4 – The QTS Network Operations Department has implemented an encrypted Virtual Private Network (VPN) that uses two factor authentication for remote connections to QTS service delivery and customer networks to protect information being transmitted over public networks.	Inspected a sample of VPN configuration settings for a sample of networks to determine whether QTS utilizes an encrypted Virtual Private Network (VPN) that uses two factor authentication for remote connections to QTS service delivery and customer networks to protect information being transmitted over public networks.	No exceptions noted.

Criteria CC5.1	Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality. (Note: Mobile systems are N/A)

QTS Description of control	KPMG's Test of controls	KPMG Results of tests
CC5.1.5 – The Information Security Department and Operations Service Center (OSC) utilize an Intrusion Detection System (IDS) to identify, log, and report potential security breaches and other incidents on QTS service delivery and customer networks. Automated notifications are generated by the IDS, routed to relevant internal and external parties if potential incidents or breaches are detected, and actions are taken as necessary to address.	Inspected a sample of identified breaches, complaints, and other incidents to determine whether breaches and other incidents are identified, logged, and reported. Inspected a sample of automated notifications to determine if they were generated by the IDS, routed to relevant internal and external parties if potential incidents or breaches are detected, and actions are taken as necessary to address.	Exceptions noted. While there were processes in place to report, evaluate and continuously monitor physical and employee/customer-reported logical security incidents, QTS Piscataway and QTS Chicago did not have a system in place over the Piscataway and Chicago internal management networks from 10/1/2016 to 7/19/2017 to identify and detect potential logical security breaches and other incidents. As a result, an exception was noted as the two networks mentioned before did not meet the portion of the criterion to identify and detect potential logical security breaches and other incidents. Please see section V for management's response to the exception.

Complementary User Entity Controls:

Not Applicable

Criteria CC5.2	New internal and external users, whose access is administered by the entity, are registered and authorized prior to being issued system credentials, and granted the ability to access the system to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.

QTS Description of control	KPMG's Test of controls	KPMG Results of tests
CC5.2.1 – Logical access is provisioned for new access and role changes for in-scope domains, operating systems, networks, databases, and applications following a management-approved access request. Provisioning requests are submitted and approved through ServiceNow and routed to appropriate personnel to perform necessary provisioning activities.	Inspected access request documentation for a sample of individuals who received logical access to the in-scope domains, operating systems, networks, databases, and applications during the period to determine whether the request was approved by management and provisioned per the request.	No exceptions noted.
CC5.2.2 – Logical access is de-provisioned for terminated individuals and role changes for in-scope domains, operating systems, networks, databases, and applications to remove logical access when it is no longer authorized. De-provisioning requests are submitted through ServiceNow and routed to appropriate personnel to perform necessary de-provisioning activities.	Inspected access de-provisioning documentation for a sample of terminated individuals to determine whether logical access to the in-scope domains, operating systems, networks, databases, and applications was removed.	No exceptions noted.

Criteria CC5.2	New internal and external users, whose access is administered by the entity, are registered and authorized prior to being issued system credentials, and granted the ability to access the system to meet the entity’s commitments and system requirements as they relate to security, availability, and confidentiality. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.

QTS Description of control	KPMG’s Test of controls	KPMG Results of tests
CC5.2.3 – The Operations Service Center (OSC) tracks employee and customer-reported incidents and/or requests, including access requests, received through the internal and customer-facing ServiceNow portal, based on impact and urgency and assigns to appropriate parties for resolution based on priority.	Inspected a sample of tickets from ServiceNow associated with customer and employee reported incidents or requests to determine whether the incidents/requests were recorded, assigned a priority classification based on impact and urgency parameters assigned to appropriate parties, and resolved.	No exceptions noted.

Complementary User Entity Controls:

a. The user entity should maintain the appropriateness of logical access for the user entity’s employees by notifying QTS when modifications (additions and removals) are necessary and reviewing access listings provided by QTS in a timely manner.

b. The user entity should notify QTS of incidents through the internal and customer-facing ServiceNow portal in a timely manner.

Criteria CC5.3	Internal and external system users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data) to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.

QTS Description of control	KPMG's Test of controls	KPMG Results of tests
CC5.3.1 – QTS Operations implements individual user network and application login credentials stored in the QTS Active Directory for the identification, authentication, and accountability of users system access.	Inspected a sample of in-scope network and application user accounts to determine whether the user IDs were assigned to individuals for ownership and accountability.	No exceptions noted.
CC5.3.2 – Network password parameters and account logon configurations covering password length, complexity, expiration, account lockout, and session timeout are implemented per QTS password specifications.	Inspected the network password configuration settings for the Jump, Compliance and Dulles domains to determine whether logon configurations are implemented covering password length, complexity, expiration, account lockout, and session timeout per the QTS password specification.	No exceptions noted.
CC5.3.3 – The QTS Network Operations Department has implemented an encrypted Virtual Private Network (VPN) that uses two factor authentication for remote connections to QTS service delivery and customer networks to protect information being transmitted over public networks.	Inspected a sample of VPN configuration settings for a sample of networks to determine whether QTS utilizes an encrypted Virtual Private Network (VPN) that uses two factor authentication for remote connections to QTS service delivery and customer networks to protect information being transmitted over public networks.	No exceptions noted.

Complementary User Entity Controls:

a) The user entity should maintain the appropriateness of logical access for the user entity's employees by notifying QTS when modifications (additions and removals) are necessary and reviewing access listings provided by QTS in a timely manner.

Criteria CC5.4	Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.

QTS Description of control	KPMG's Test of controls	KPMG Results of tests
CC5.4.1 – Annually, the Information Security Department initiates a review of user access to in scope domains, operating systems, networks, databases and applications to confirm appropriateness of access and identify any necessary changes. Identified changes are routed through ServiceNow for provisioning changes.	Inspected the annual review of logical access to the in-scope domains, operating systems, networks, databases, and applications to determine whether the review was completed, the appropriateness of user access was assessed by management and identified changes were actioned and resolved.	No exceptions noted.
CC5.4.2 – Logical access is provisioned for new access and role changes for in-scope domains, operating systems, networks, databases, and applications following a management-approved access request. Provisioning requests are submitted and approved through ServiceNow and routed to appropriate personnel to perform necessary provisioning activities.	Inspected access request documentation for a sample of individuals who received logical access to the in-scope domains, operating systems, networks, databases, and applications during the period to determine whether the request was approved by management and provisioned per the request.	No exceptions noted.

Criteria CC5.4	Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.	
QTS Description of control	**KPMG's Test of controls**	**KPMG Results of tests**
CC5.4.3 – Logical access is de-provisioned for terminated individuals and role changes for in-scope domains, operating systems, networks, databases, and applications to remove logical access when it is no longer authorized. De-provisioning requests are submitted through ServiceNow and routed to appropriate personnel to perform necessary de-provisioning activities.	Inspected access de-provisioning documentation for a sample of terminated individuals to determine whether logical access to the in-scope domains, operating systems, networks, databases, and applications was removed.	No exceptions noted.
CC5.4.4 – Semi-Annually, the Information Security Department initiates a review of internal badge holder physical access, generated from the physical security badge application, to confirm appropriateness of access and identify any necessary changes. Identified changes are routed through ServiceNow for provisioning changes.	Inspected documentation for a sample semi-annual review of internal badge holder physical access to computer resources and system administrator access to the security badging system to determine whether the review was completed, the appropriateness of user access was assessed by management and identified changes were actioned and resolved.	No exceptions noted.

Criteria CC5.4	Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to meet the entity’s commitments and system requirements as they relate to security, availability, and confidentiality.

QTS Description of control	KPMG’s Test of controls	KPMG Results of tests
CC5.4.5 – Physical access to facilities is provisioned for new access and role changes following a management-approved access request. Provisioning request are submitted and approved through ServiceNow and routed to appropriate personnel to perform necessary provisioning activities.	Inspected tickets from the ticketing system for a sample of individuals granted new or changed physical access to computer resources to determine whether the access was documented and approved by an authorized individual (for customers, an individual included on the security roster) prior to access being granted.	No exceptions noted.
CC5.4.6 – Physical access to computer resources is de-provisioned for terminations and role changes when it is no longer authorized. De-provisioning requests are submitted through ServiceNow and routed to appropriate personnel to perform necessary de-provisioning activities.	Inspected the User De-Provisioning form and security badging system access settings for a sample of terminated individuals to determine whether access was removed following notification of termination or a role change.	No exceptions noted.

Complementary User Entity Controls:

a. The user entity should maintain the appropriateness of logical and physical access for the user entity’s employees by notifying QTS when modifications (additions and removals) are necessary and reviewing access listings provided by QTS in a timely manner.

Criteria CC5.5	Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations as well as sensitive system components within those locations) is restricted to authorized personnel to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.

QTS Description of control	KPMG's Test of controls	KPMG Results of tests
CC5.5.1 – QTS facilities are equipped with fences and/or walls located around the perimeter of the building, where applicable, to prevent unauthorized access.	Observed in-scope facilities to determine whether the facilities are equipped with fences and/or walls located around the perimeter of the building to prevent unauthorized access, where applicable.	No exceptions noted.
CC5.5.2 – QTS Facilities are equipped with guard stands located at the entrance of the building to prevent unauthorized access to the surrounding secured perimeter.	Observed in-scope facilities to determine whether the facilities are equipped with guard stands located at the entrance of the building to prevent unauthorized access to the surrounding secured perimeter.	No exceptions noted.
CC5.5.3 – The QTS Physical Security Department conducts security patrols by inspecting the property and reporting any incidents to supervisors and/or emergency services. The patrols are performed per QTS procedures.	Observed the process for the Security Department to conduct the property security patrol inspections. Inspected the physical security procedures document and a sample of security log reports to determine whether the property was regularly inspected and any incidents noted were reported.	No exceptions noted.
CC5.5.4 – The QTS Security Office monitors video surveillance from security cameras installed within and surrounding the building 24x7x365 to monitor activities throughout the facility.	Observed in-scope facilities to determine whether the facilities are equipped with security cameras for video surveillance of areas in and around the building, and the video is monitored by Security Officers.	No exceptions noted.

Criteria CC5.5	Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations as well as sensitive system components within those locations) is restricted to authorized personnel to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.

QTS Description of control	KPMG's Test of controls	KPMG Results of tests
CC5.5.5 – The Security Office checks in all visitors based on their official government-issued picture identification and tracks the identification information in the Visitor Management System. A visitor badge with this information is provided to the visitor and must be worn at all times to clearly identify the visitor. Visitors are escorted by authorized personnel while in sensitive areas.	Inspected QTS' physical access policy to determine that visitors are required to check in with security, show official government-issued picture identification, wear and display a visitor badge, sign the visitors log prior to accessing restricted areas, and must be escorted at all times by authorized personnel. Observed the process for checking in data center visitors at in-scope facilities to determine whether visitors to the data center must show government-issued picture identification, wear and display a visitor badge, sign the visitors log prior to accessing restricted areas, and must be escorted at all times by authorized personnel.	No exceptions noted.
CC5.5.6 – The QTS Facilities Department restricts physical access to sensitive data center areas to authorized personnel using holding rooms requiring two-factor authentication.	Inspected the physical security procedures document to determine if physical access to sensitive data center areas is restricted to authorized personnel using holding rooms requiring two-factor authentication. Observed access to specific data center areas at in-scope facilities to determine whether they are restricted through the use of two-door holding rooms that require two-factor authentication to gain access to the applicable data center floor.	No exceptions noted.
CC5.5.7 – Physical access to facilities is provisioned for new access and role changes following a management-approved access request. Provisioning request are submitted and approved through ServiceNow and routed to appropriate personnel to perform necessary provisioning activities.	Inspected tickets from ServiceNow for a sample of individuals granted new or changed physical access to computer resources to determine whether the access was documented and approved by an authorized individual (for customers, an individual included on the security roster) prior to access being granted.	No exceptions noted.

Criteria CC5.5	Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations as well as sensitive system components within those locations) is restricted to authorized personnel to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.

QTS Description of control	**KPMG's Test of controls**	**KPMG Results of tests**
CC5.5.8 – Physical access to computer resources is de-provisioned for terminations and role changes when it is no longer authorized. De-provisioning requests are submitted through ServiceNow and routed to appropriate personnel to perform necessary de-provisioning activities.	Inspected the User De-Provisioning form and security badging system access settings for a sample of terminated individuals to determine whether access was removed following notification of termination or a role change. Note* The customer removal process is tested at control CC5.5.9.	No exceptions noted.
CC5.5.9 – The Operations Service Center (OSC) tracks employee and customer-reported incidents and/or requests, including access requests, received through the internal and customer-facing ServiceNow portal, based on impact and urgency and assigns to appropriate parties for resolution based on priority.	Inspected a sample of tickets from ServiceNow associated with customer and employee reported incidents or requests to determine whether the incidents/requests were recorded, assigned a priority classification based on impact and urgency parameters assigned to appropriate parties, and resolved.	No exceptions noted.
CC5.5.10 – The QTS Facilities Department secures data center cabinets, cages, and suites to restrict access to authorized personnel through the use of combination locks, traditional lock and key mechanisms, electronic readers and/or infrared beams.	Observed access to data center cabinets, cages and suites at in-scope facilities to determine whether they are secured through the use of combination locks, traditional lock & key mechanisms, electronic readers and/or infrared beams.	No exceptions noted.

Criteria CC5.5	Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations as well as sensitive system components within those locations) is restricted to authorized personnel to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.

QTS Description of control	KPMG's Test of controls	KPMG Results of tests
CC5.5.11 – The QTS Facilities Department securely retains log and video records of data center physical access events onsite for at least three months on a local database to allow for subsequent review of security events. Backups are also securely stored offsite for disaster recovery for the duration of the retention period.	Inspected sample log records and video records of data center access events from the in-scope facilities to determine that these are securely retained for at least three months locally, and securely stored offsite for disaster recovery for the duration of the retention period.	No exceptions noted.
CC5.5.12 – Semi-Annually, the Information Security Department initiates a review of internal badge holder physical access, generated from the physical security badge application, to confirm appropriateness of access and identify any necessary changes. Identified changes are routed through ServiceNow for provisioning changes.	Inspected documentation for a sample semi-annual review of internal badge holder physical access to computer resources and system administrator access to the security badging system to determine whether the review was completed, the appropriateness of user access was assessed by management and identified changes were actioned and resolved.	No exceptions noted.

Complementary User Entity Controls:

a. The user entity should maintain the appropriateness of physical access for the user entity's employees by notifying QTS when modifications (additions and removals) are necessary and reviewing access listings provided by QTS in a timely manner.

b. The user entity should maintain appropriate security of traditional lock and keys, combination lock codes, and/or electronic badges retained by the user entity's employees.

Criteria CC5.6	Logical access security measures have been implemented to protect against security, availability, and confidentiality threats from sources outside the boundaries of the system to meet the entity's commitments and system requirements.

QTS Description of control	KPMG's Test of controls	KPMG Results of tests
CC5.6.1 – The QTS Network Operations Department restricts traffic to authorized inbound and outbound traffic through the use of firewalls to protect networks in accordance with QTS firewall configuration standards. Firewall configuration standards are set to appropriately restrict unauthorized user access.	Inspected firewall configurations to determine whether QTS has firewalls in place to restrict inbound and outbound traffic or unauthorized user access, and that settings are in conformance with QTS Firewall configuration standards or per customer specifications.	No exceptions noted.
CC5.6.2 – The QTS Network Operations Department has implemented an encrypted Virtual Private Network (VPN) that uses two factor authentication for remote connections to QTS service delivery and customer networks to protect information being transmitted over public networks.	Inspected a sample of VPN configuration settings for a sample of networks to determine whether QTS utilizes an encrypted Virtual Private Network (VPN) that uses two factor authentication for remote connections to QTS service delivery and customer networks to protect information being transmitted over public networks.	No exceptions noted.

Complementary User Entity Controls:

Not Applicable

<table>
<tr><td>Criteria CC5.7</td><td colspan="2">The transmission, movement, and removal of information is restricted to authorized internal and external users and processes, and is protected during transmission, movement, or removal enabling the entity to meet its commitments and requirements as they relate to security, availability, and confidentiality.
(Note: QTS does not handle the transmission of user entity information.)</td></tr>
<tr><th>QTS Description of control</th><th>KPMG’s Test of controls</th><th>KPMG Results of tests</th></tr>
<tr><td>CC5.7.1 –
The QTS Operations Department encrypts all removable backup data so that data is protected.</td><td>Inspected backup media system configurations to determine whether backup media is encrypted.</td><td>No exceptions noted.</td></tr>
<tr><td colspan="3">Complementary User Entity Controls:
Not Applicable</td></tr>
</table>

Criteria CC5.8	Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity’s commitments and system requirements as they relate to security, availability, and confidentiality.	
QTS Description of control	**KPMG’s Test of controls**	**KPMG Results of tests**
CC5.8.1 – The QTS Operations Department implements and configures the Symantec anti-virus software to monitor and prevent the activation of unwanted and malicious software in the environment for all QTS systems.	Inspected system configurations to determine whether the antivirus software is configured to query the antivirus repository daily to retrieve the latest antivirus definitions. Inspected results for a sample of weeks to determine that antivirus scans are performed weekly and that exception reports are generated based on detection of computer viruses, malicious code, and unauthorized software as applicable to QTS systems.	No exceptions noted.
Complementary User Entity Controls: Not Applicable		

Criteria CC6.0	**Common Criteria Related to System Operations: The criteria relevant to how the organization manages the execution of system procedures and detects and mitigates processing deviations, including logical and physical security deviations, to meet the objective(s) of the principle(s) addressed in the engagement.**

Criteria CC6.1	Vulnerabilities of system components to security, availability, and confidentiality breaches and incidents due to malicious acts, natural disasters, or errors are identified, monitored and evaluated and countermeasures are designed, implemented and operated to compensate for known and newly identified vulnerabilities to meet the entity’s commitments and system requirements as they relate to security, availability, and confidentiality.	
QTS Description of control	**KPMG’s Test of controls**	**KPMG Results of tests**
CC6.1.1 – Annually, the Information Security Department performs a comprehensive vulnerability scan to identify potential risks to system security and confidentiality. Risks are reviewed and remediation plans are developed, reviewed by management, and mitigation completed	Inspected the results of the annual comprehensive vulnerability scans to determine whether: a. Scans and testing are performed annually to identify potential risks to system security and confidentiality; b. Identified risks are reviewed and evaluated against the defined QTS security and confidentiality policies, service level agreements, and other QTS obligations; and; c. The assessment results and remediation plans are reviewed, approved, and monitored to determine completion of mitigation by Line of Business Owners and the ISO team.	No exceptions noted.

Criteria CC6.1	Vulnerabilities of system components to security, availability, and confidentiality breaches and incidents due to malicious acts, natural disasters, or errors are identified, monitored and evaluated and countermeasures are designed, implemented and operated to compensate for known and newly identified vulnerabilities to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.

QTS Description of control	KPMG's Test of controls	KPMG Results of tests
CC6.1.2 – The Information Security Department and Operations Service Center (OSC) utilize an Intrusion Detection System (IDS) to identify, log, and report potential security breaches and other incidents on QTS service delivery and customer networks. Automated notifications are generated by the IDS, routed to relevant internal and external parties if potential incidents or breaches are detected, and actions are taken as necessary to address.	Inspected a sample of identified breaches, complaints, and other incidents to determine whether breaches and other incidents are identified, logged, and reported. Inspected a sample of automated notifications to determine if they were generated by the IDS, routed to relevant internal and external parties if potential incidents or breaches are detected, and actions are taken as necessary to address.	Exceptions noted. Please see the exception write-up in control CC5.1.5.
CC6.1.3 – The QTS Operations Department monitors the availability and performance of the QTS service delivery networks and systems 24x7x365 using the CA Unified Infrastructure Management monitoring tool which sends automated notifications to customers and/or QTS for critical events outside an acceptable range.	Inspected a sample of CA Unified Infrastructure Management internal automated alerts to determine whether alerts are generated when critical events or potential system or network disruption is detected. Inspected corresponding tickets to determine whether a ticket is generated, as appropriate, and routed to appropriate parties for resolution.	No exceptions noted.

Criteria CC6.1	Vulnerabilities of system components to security, availability, and confidentiality breaches and incidents due to malicious acts, natural disasters, or errors are identified, monitored and evaluated and countermeasures are designed, implemented and operated to compensate for known and newly identified vulnerabilities to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.

QTS Description of control	KPMG's Test of controls	KPMG Results of tests
CC6.1.4 – The Information Security Department has documented procedures available to internal users for the identification, notification and escalation of incidents via ServiceNow so that breaches, complaints and incidents are handled and communicated to the relevant internal and external parties.	Inspected system availability, breach, and complaint procedures to determine whether QTS has documented procedures for the identification, notification and escalation of possible system availability issues, security breaches, confidentiality breaches, complaints and other incidents.	No exceptions noted.
CC6.1.5 – The Operations Service Center (OSC) tracks employee and customer-reported incidents and/or requests, including access requests, received through the internal and customer-facing ServiceNow portal, based on impact and urgency and assigns to appropriate parties for resolution based on priority.	Inspected a sample of tickets from ServiceNow associated with customer and employee reported incidents or requests to determine whether the incidents/requests were recorded, assigned a priority classification based on impact and urgency parameters assigned to appropriate parties, and resolved.	No exceptions noted.

Criteria CC6.1	Vulnerabilities of system components to security, availability, and confidentiality breaches and incidents due to malicious acts, natural disasters, or errors are identified, monitored and evaluated and countermeasures are designed, implemented and operated to compensate for known and newly identified vulnerabilities to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.

QTS Description of control	KPMG's Test of controls	KPMG Results of tests
CC6.1.6 – Weekly, the Operations Service Center reviews open tickets in ServiceNow to follow up on the open incidents and requests for customer and business needs.	Inspected the Open Incident Reports for a sample of weeks to determine whether open tickets were reviewed and followed up on by the OSC as needed.	No exceptions noted.

Complementary User Entity Controls:

a) The user entity should review automated notifications that are generated and provided for certain events as specified by the user entity and notify QTS where further action is needed.

Criteria CC6.2	Security, availability, and confidentiality incidents, including logical and physical security breaches, failures, and identified vulnerabilities, are identified, reported to appropriate personnel, and acted on in accordance with established incident response procedures to meet the entity’s commitments and system requirements.

QTS Description of control	KPMG’s Test of controls	KPMG Results of tests
CC6.2.1 – The Operations Service Center (OSC) tracks employee and customer-reported incidents and/or requests, including access requests, received through the internal and customer-facing ServiceNow portal, based on impact and urgency and assigns to appropriate parties for resolution based on priority.	Inspected a sample of tickets from ServiceNow associated with customer and employee reported incidents or requests to determine whether the incidents/requests were recorded, assigned a priority classification based on impact and urgency parameters assigned to appropriate parties, and resolved.	No exceptions noted.
CC6.2.2 Weekly, the Operations Service Center reviews open tickets in ServiceNow to follow up on the open incidents and requests for customer and business needs.	Inspected the Open Incident Reports for a sample of weeks to determine whether open tickets were reviewed and followed up on by the OSC as needed for resolution.	No exceptions noted.

Criteria CC6.2	Security, availability, and confidentiality incidents, including logical and physical security breaches, failures, and identified vulnerabilities, are identified, reported to appropriate personnel, and acted on in accordance with established incident response procedures to meet the entity’s commitments and system requirements.

QTS Description of control	KPMG’s Test of controls	KPMG Results of tests
CC6.2.3 – The Operations Service Center (OSC) coordinates with relevant line of business management so that appropriate actions are taken to address high severity and major incidents. An after action report, identifying the resolution, root causes(s), and change management processes initiated to avoid future occurrences, are documented.	Inspected a sample of high severity and major incidents to determine whether an after action report, identifying the resolution, root causes(s), and change management processes initiated to avoid future occurrences, were documented.	No exceptions noted.

Complementary User Entity Controls:

Not Applicable

Criteria CC7.0	**Common Criteria Related to Change Management: The criteria relevant to how the organization identifies the need for changes to the system, makes the changes following a controlled change management process, and prevents unauthorized changes from being made to meet the criteria for the principle(s) addressed in the engagement.**

Criteria CC7.1	The entity's commitments and system requirements, as they relate to security, availability, and confidentiality are addressed during the system development lifecycle including the authorization, design, acquisition, implementation, configuration, testing, modification, and maintenance of system components.

QTS Description of control	KPMG's Test of controls	KPMG Results of tests
CC7.1.1 – The QTS Product Development Department follows an established SDLC methodology consistent with the defined QTS security, availability and confidentiality policies and framework that governs the design, acquisition, implementation, configuration, testing, maintenance, modification and management of infrastructure and software components.	Inspected the SDLC Methodology Policies and Procedures, to determine whether QTS has established a Systems Development Life Cycle (SDLC) methodology consistent with the defined QTS security, availability and confidentiality policies and framework that governs the design, acquisition, implementation, configuration, testing, maintenance, modification and management of infrastructure and software components.	No exceptions noted.
CC7.1.2 – The QTS Change Team has established change management policies and procedures dictating required steps in the change management process so that necessary change management activities are performed prior to implementation of changes.	Inspected the QTS change management policies and procedures to determine if there are defined policies and procedures in place to govern systems development and maintenance activities.	No exceptions noted.

Criteria CC7.1	The entity’s commitments and system requirements, as they relate to security, availability, and confidentiality are addressed during the system development lifecycle including the authorization, design, acquisition, implementation, configuration, testing, modification, and maintenance of system components.	
QTS Description of control	**KPMG’s Test of controls**	**KPMG Results of tests**
CC7.1.3 – The QTS Change Team requires that all changes are documented, tested where applicable and approved for critical applications, servers and databases prior to production implementation so that only authorized changes are implemented. Documentation and approvals are tracked through workflow in ServiceNow.	Inspected tickets from ServiceNow for a sample of changes to critical applications, servers and databases to determine whether the changes were planned, tested (where applicable) and approved prior to production implementation. Inspected tickets from ServiceNow for a sample of changes to critical applications, servers and databases to determine whether the changes were implemented into production by authorized personnel.	No exceptions noted.
Complementary user entity controls: Not Applicable		

Criteria CC7.2	Infrastructure, data, software, and policies and procedures are updated as necessary to remain consistent with the entity's commitments and system requirements as they relate to security, availability, and confidentiality. (Note: There are no data components in scope for this report.)

QTS Description of control	KPMG's Test of controls	KPMG Results of tests
CC7.2.1 – Annually, the QTS Operations Department reviews infrastructure and software components, including system configurations, against the defined QTS Security, Availability, and Confidentiality policies and current Service-Level Agreements for consistency. Identified inconsistencies are documented and routed to appropriate parties for resolution.	Inspected the annual Infrastructure and software components assessment to determine whether: a. The infrastructure, data and software components were evaluated against the defined QTS security, availability, and confidentiality policies and current service-level agreements for consistency b. The assessment was reviewed by Management and identified inconsistencies documented and routed to appropriate parties for resolution.	No exceptions noted.
CC7.2.2 – The QTS Corporate Policy Committee oversees adherence to the QTS policy management methodology for the QTS policy set to determine that QTS policy is in compliance with the established methodology. The Committee reviews to determine whether policies identify owners and scope, are updated as required, and are reviewed annually at a minimum prior to publishing to the QTS policy set per the Document Governance specification.	Inspected QTS policies, procedures and specifications to determine whether the documents have been established that: a) Address the security, availability, and confidentiality of its services b) Identify policy owners and scope c) Have been reviewed annually and updated as necessary and, d) Any new/significantly changed policies have been communicated to all users and available on the company's intranet.	No exceptions noted.

Complementary User Entity Controls:

a) The user entity should review information provided by QTS regarding system maintenance and patching updates available for its environment and request any updates it deems necessary.

Criteria CC7.3	Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and are monitored to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.	
QTS Description of control	**KPMG's Test of controls**	**KPMG Results of tests**
CC7.3.1 – The Operations Service Center (OSC) coordinates with relevant line of business management so that appropriate actions are taken to address high severity and major incidents. An after action report, identifying the resolution, root causes(s), and change management processes initiated to avoid future occurrences, are documented.	Inspected a sample of high severity and major incidents to determine whether an after action report, identifying the resolution, root causes(s), and change management processes initiated to avoid future occurrences, were documented.	No exceptions noted.
Complementary User Entity Controls: a) The user entity should notify QTS of incidents through the internal and customer-facing ServiceNow portal in a timely manner.		

Criteria CC7.4	Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented to meet the entity's security, availability, and confidentiality commitments and system requirements.

QTS Description of control	KPMG's Test of controls	KPMG Results of tests
CC7.4.1 – The QTS Change Team has established change management policies and procedures dictating required steps in the change management process so that necessary change management activities are performed prior to implementation of changes.	Inspected the QTS change management policies and procedures to determine if there are defined policies and procedures in place to govern systems development and maintenance activities.	No exceptions noted.
CC7.4.2 – The QTS Change Team requires that all changes are documented, tested where applicable and approved for critical applications, servers and databases prior to production implementation so that only authorized changes are implemented. Documentation and approvals are tracked through workflow in ServiceNow.	Inspected tickets from ServiceNow for a sample of changes to critical applications, servers and databases to determine whether the changes were planned, tested (where applicable) and approved prior to production implementation. Inspected tickets from ServiceNow for a sample of changes to critical applications, servers and databases to determine whether the changes were implemented into production by authorized personnel.	No exceptions noted.
CC7.4.3 – The QTS Change Team has a formal process in place to approve emergency change requests, through the approval of two line of business owners prior to production implementation, so that only authorized changes are implemented. Documentation and approvals are tracked through workflow in ServiceNow.	Inspected tickets from ServiceNow for a sample of emergency change requests to determine whether the changes were approved by two LOB Senior Manager level (or higher) executives prior to production implementation.	No exceptions noted.

Criteria CC7.4	Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented to meet the entity's security, availability, and confidentiality commitments and system requirements.

QTS Description of control	**KPMG's Test of controls**	**KPMG Results of tests**
CC7.4.4 – The QTS Change Team completes a post implementation review of all failed changes in order to assign the necessary steps for resolution.	Inspected tickets from ServiceNow for a sample of QTS failed changes to determine whether the Internal Change Advisory Board (CAB) completed the post-implementation review to assign the necessary step for resolution.	No exceptions noted.

Complementary User Entity Controls:

a The user entity should review information provided by QTS regarding system maintenance and patching updates available for its environment and request any updates it deems necessary.

b The user entity should perform user acceptance testing on any system maintenance and patching updates applicable to its environment upon notification by QTS.

Criteria A1.1	Current processing capacity and usage are maintained, monitored, and evaluated to manage capacity demand and to enable the implementation of additional capacity to help meet the entity’s availability commitments and system requirements.

QTS Description of control	KPMG’s Test of controls	KPMG Results of tests
A1.1.1 – The QTS Operations Department monitors the availability and performance of the QTS service delivery networks and systems 24x7x365 using the CA Unified Infrastructure Management monitoring tool which sends automated notifications to customers and/or QTS for critical events outside an acceptable range.	Inspected a sample of CA Unified Infrastructure Management internal automated alerts to determine whether alerts are generated when critical events or potential system or network disruption is detected. Inspected corresponding tickets to determine whether a ticket is generated, as appropriate, and routed to appropriate parties for resolution.	No exceptions noted.

Complementary User Entity Controls:

Not Applicable

Criteria A1.2	Environmental protections, software, data backup processes, and recovery infrastructure are authorized, designed, developed, implemented, operated, approved, maintained, and monitored to meet entity's availability commitments and system requirements.

QTS Description of control	KPMG's Test of controls	KPMG Results of tests
A1.2.1 – QTS facilities are equipped with fire detection and suppression systems so that QTS is able to meet availability commitments and requirements.	Observed the data centers at in-scope facilities to determine whether the data centers have fire detection and suppression elements in place and fire extinguishers have been installed.	No exceptions noted.
A1.2.2 – QTS facilities are equipped with redundant mechanical and electrical infrastructure such as uninterruptible power supplies (UPS) and diesel generators so that QTS is able to meet availability commitments and requirements.	Observed the data centers at in-scope facilities to determine whether the data centers are equipped with redundant mechanical and electrical infrastructure such as uninterruptible power supplies (UPS) and diesel generators.	No exceptions noted.
A1.2.3 – The QTS Facilities Department monitors heating, ventilation and air conditioning (HVAC) elements for the data center and supporting infrastructure rooms and takes necessary action for predefined monitoring alerts per QTS procedures.	Inspected the HVAC monitoring procedures document and a sample of monitoring alerts for the in-scope facilities to determine whether the data centers have alerts that are triggered when predefined events occur or out-of-range thresholds are reached for heating, ventilation, and air conditioning ("HVAC") elements for areas housing electronic equipment in place.	No exceptions noted.

Criteria A1.2	Environmental protections, software, data backup processes, and recovery infrastructure are authorized, designed, developed, implemented, operated, approved, maintained, and monitored to meet entity's availability commitments and system requirements.

QTS Description of control	KPMG's Test of controls	KPMG Results of tests
A1.2.4 – The QTS Facilities Department conducts routine inspections of all fire detection and suppression systems and performs quarterly, semi-annual and annual checks per National Fire Protection Association (NFPA), Federal, State and Local requirements to determine that fire detection and suppression systems are able to meet availability commitments and requirements.	Inspected documentation for a sample of the routine inspections and the quarterly, semi-annual and annual checks of all fire detection and suppression systems to determine whether the inspections and checks were performed in the period.	No exceptions noted.
A1.2.5 – The QTS Facilities Department conducts critical infrastructure inspections of the generators, UPS and battery banks and performs generator load testing and generator start-up time testing in accordance with the critical maintenance plan located in Emaint Maintenance Software so that the facility infrastructure is able to meet the availability commitments and requirements.	Inspected documentation for a sample of the critical infrastructure routine inspections, generator load testing and generator start-up time testing to determine whether the inspections and testing of the generators, UPS and battery banks were performed in accordance with the critical maintenance plan.	No exceptions noted.

Criteria A1.2	Environmental protections, software, data backup processes, and recovery infrastructure are authorized, designed, developed, implemented, operated, approved, maintained, and monitored to meet entity's availability commitments and system requirements.

QTS Description of control	KPMG's Test of controls	KPMG Results of tests
A1.2.6 – Daily, the QTS Facilities Department inspects and records, in the facility monitoring system, critical facility infrastructure readings and metrics for mechanical and electrical infrastructure so that facility infrastructure is able to meet availability commitments and requirements.	Observed QTS personnel monitor critical infrastructure components at in-scope facilities to determine whether readings and metrics are regularly inspected, documented and recorded in a facility log report. Inspected a sample of facility log reports to determine whether critical facility infrastructure readings are regularly inspected, documented and recorded in a facility log report.	No exceptions noted.
A1.2.7 – The QTS Facilities Department maintains, annually reviews, authorizes, approves and updates a critical maintenance plan in the Emaint maintenance software that is followed so that facility infrastructure is able to meet availability commitments and requirements per QTS procedures.	Inspected data center maintenance plans to determine whether: a. A plan exists that addresses the maintenance of critical equipment that supports QTS' key operations and b. The plan is updated/reviewed/approved annually.	No exceptions noted.

Criteria A1.2	Environmental protections, software, data backup processes, and recovery infrastructure are authorized, designed, developed, implemented, operated, approved, maintained, and monitored to meet entity's availability commitments and system requirements.	
QTS Description of control	**KPMG's Test of controls**	**KPMG Results of tests**
A1.2.8 – The QTS Operations Department performs incremental and full backups on program and data files which are maintained on tape libraries and/or disk storage. Failures are identified, logged, and routed to appropriate parties for resolution based on impact and urgency parameters.	Inspected the backup schedule configurations to determine whether incremental and full backups are scheduled for critical program and data files. Inspected the system configuration to determine whether the system is setup to notify appropriate personnel of backup failures. Inspected system logs, email notifications or tickets for a sample of backup failures to determine whether backups were identified, logged, monitored and resolved by appropriate parties.	No exceptions noted.
A1.2.9 – As needed, the QTS Operations Department stores backup media with an offsite third party vendor to meet the defined system availability and related security policies.	Inspected a sample of backup inventory tickets from a third party vendor to determine whether backup media is stored offsite consistent with the defined system availability and related security policies and contractual agreements.	No exceptions noted.
A1.2.10 – Quarterly, the QTS Operations Department tests data backups for recoverability to determine that data can be successfully recovered from backups.	Inspected a sample of backup recoverability tests performed to determine whether data backups are quarterly tested for recoverability.	No exceptions noted.
Complementary User Entity Controls: Not Applicable		

Criteria A1.3	Recovery plan procedures supporting system recovery are tested to help meet the entity's availability commitments and system requirements.	
QTS Description of control	**KPMG's Test of controls**	**KPMG Results of tests**
A1.3.1 – Annually, the Business Continuity Department and line of business owners' review, update, and approve QTS Business Continuity procedures to determine that accurate processes are in place to meet defined availability, security, and contractual requirements.	Inspected QTS Business Continuity Procedures to determine if they are reviewed annually by the Business Continuity Department and line of business owners, and that processes are in place to meet defined availability, security, and contractual requirements.	No exceptions noted.
A1.3.2 – Annually, the Business Continuity Department and the line of business owners test the business contingency plans retained in SharePoint to determine that the plans are sufficient to allow QTS to meet defined availability, security, and contractual requirements in the case of a disaster.	Inspected supporting documentation to determine whether business contingency plans are tested annually to determine that the plans are sufficient to allow QTS to meet defined availability, security, and contractual requirements in the case of a disaster.	No exceptions noted.
Complementary User Entity Controls: Not Applicable		

Criteria C1.1	Confidential information is protected during the system design, development, testing, implementation, and change processes to meet the entity’s confidentiality commitments and system requirements.

QTS Description of control	KPMG’s Test of controls	KPMG Results of tests
C1.1.1 – The Information Security Department has documented procedures so that confidentiality policies are being implemented and upheld.	Inspected evidence of system procedures (such as access administration, network configuration) to determine whether QTS has established system procedures for the confidentiality of inputs, data processing, and outputs that are consistent with the documented confidentiality policies.	No exceptions noted.
C1.1.2 – The QTS Product Development Department has established policies to protect data and meet confidentiality commitments and requirements during system design, development, testing, and implementation.	Inspected QTS policies to determine whether policies have been established by management to address the use of data subject to confidentiality requirements during system design, development, testing, and implementation. Inspected system evidence of the production, development and test environments and noted that the production environment is separated from the development and test environments to protect data and meet confidentiality commitments and requirements during system design, development, testing, and implementation.	No exceptions noted.

Complementary User Entity Controls:

Not Applicable

Criteria C1.2	Confidential information within the boundaries of the system is protected against unauthorized access, use, and disclosure during input, processing, retention, output, and disposition to meet the entity's confidentiality commitments and system requirements.

QTS Description of control	KPMG's Test of controls	KPMG Results of tests
C1.2.1 – The Information Security Department has documented procedures so that confidentiality policies are being implemented and upheld.	Inspected evidence of system procedures (such as access administration, network configuration) to determine whether QTS has established system procedures for the confidentiality of inputs, data processing, and outputs that are consistent with the documented confidentiality policies.	No exceptions noted.
C1.2.2 – The QTS Operations Department encrypts all removable backup data so that data is protected.	Inspected backup media system configurations to determine whether backup media is encrypted.	No exceptions noted.
C1.2.3 – The QTS Product Development Department has established policies to protect data and meet confidentiality commitments and requirements during system design, development, testing, and implementation.	Inspected QTS policies to determine whether policies have been established by management to address the use of data subject to confidentiality requirements during system design, development, testing, and implementation. Inspected system evidence of the production, development and test environments and noted that the production environment is separated from the development and test environments to protect data and meet confidentiality commitments and requirements during system design, development, testing, and implementation.	No exceptions noted.

Criteria C1.2	Confidential information within the boundaries of the system is protected against unauthorized access, use, and disclosure during input, processing, retention, output, and disposition to meet the entity’s confidentiality commitments and system requirements.

QTS Description of control	KPMG’s Test of controls	KPMG Results of tests
C1.2.4 – QTS communicates to customers’ roles and responsibilities and security, availability, and confidentiality commitments within the Data Center handbook located on the Customer Portal. The Customer Portal lists the customer's responsibilities and process to report operational failures, incidents, problems, concerns and complaints.	Inspected QTS' customer portal to determine whether the data center handbook is available and customers' responsibilities, which include responsibility for reporting operational failures, incidents, problems, concerns and complaints, and the process for doing so, are also described in the customer portal. Inspected a sample of Data center handbooks to determine whether the entity’s security, availability, and confidentiality commitments, roles and responsibilities were included.	No exceptions noted.

Complementary User Entity Controls:

Not Applicable

Criteria C1.3	Access to confidential information from outside the boundaries of the system and disclosure of confidential information is restricted to authorized parties to meet the entity's confidentiality commitments and system requirements.

QTS Description of control	KPMG's Test of controls	KPMG Results of tests
C1.3.1 – QTS Operations implements individual user network and application login credentials stored in the QTS Active Directory for the identification, authentication, and accountability of users' system access.	Inspected a sample of in-scope network, and application user accounts to determine whether the user IDs were assigned to individuals for ownership and accountability.	No exceptions noted.
C1.3.2 – Network password parameters and account logon configurations covering password length, complexity, expiration, account lockout, and session timeout are implemented per QTS password specifications.	Inspected the network password configuration settings for the Jump, Compliance and Dulles domains to determine whether logon configurations are implemented covering password length, complexity, expiration, account lockout, and session timeout per the QTS password specification.	No exceptions noted.
C1.3.3 – The QTS Operations Department encrypts all removable backup data so that data is protected.	Inspected backup media system configurations to determine whether backup media is encrypted.	No exceptions noted.

Criteria C1.3	Access to confidential information from outside the boundaries of the system and disclosure of confidential information is restricted to authorized parties to meet the entity’s confidentiality commitments and system requirements.

QTS Description of control	KPMG’s Test of controls	KPMG Results of tests
C1.3.4 – The QTS Network Operations Department restricts traffic to authorized inbound and outbound traffic through the use of firewalls to protect networks in accordance with QTS firewall configuration standards. Firewall configuration standards are set to appropriately restrict unauthorized user access.	Inspected firewall configurations to determine whether QTS has firewalls in place to restrict inbound and outbound traffic or unauthorized user access, and that settings are in conformance with QTS Firewall configuration standards or per customer specifications.	No exceptions noted.
C1.3.5 – The QTS Network Operations Department has implemented an encrypted Virtual Private Network (VPN) that uses two factor authentication for remote connections to QTS service delivery and customer networks to protect information being transmitted over public networks.	Inspected a sample of VPN configuration settings for a sample of networks to determine whether QTS utilizes an encrypted Virtual Private Network (VPN) that uses two factor authentication for remote connections to QTS service delivery and customer networks to protect information being transmitted over public networks.	No exceptions noted.

Criteria C1.3	Access to confidential information from outside the boundaries of the system and disclosure of confidential information is restricted to authorized parties to meet the entity's confidentiality commitments and system requirements.

QTS Description of control	KPMG's Test of controls	KPMG Results of tests
C1.3.6 – The QTS Legal Department obtains information sharing agreements with vendors and third parties such as non-disclosure agreements, master terms and conditions, and/or master agreements of professional services. These agreements, retained in the QTS SharePoint, outline confidentiality commitments between QTS and vendors/third parties to determine that QTS data is kept confidential.	Inspected a sample of new or amended agreements during the period to determine whether the documentation contains confidentiality commitments between QTS and vendors/third parties to determine that QTS data is kept confidential.	No exceptions noted.
Complementary User Entity Controls: Not Applicable		

Criteria C1.4	The entity obtains confidentiality commitments that are consistent with the entity's confidentiality system requirements, from vendors and other third parties whose products and services are part of the system and have access to confidential information.

QTS Description of control	KPMG's Test of controls	KPMG Results of tests
C1.4.1 – The QTS Legal Department obtains information sharing agreements with vendors and third parties such as non-disclosure agreements, master terms and conditions, and/or master agreements of professional services. These agreements, retained in the QTS SharePoint, outline confidentiality commitments between QTS and vendors/third parties to determine that QTS data is kept confidential.	Inspected a sample of new or amended agreements during the period to determine whether the documentation contains confidentiality commitments between QTS and vendors/third parties to determine that QTS data is kept confidential.	No exceptions noted.
Complementary User Entity Controls: Not Applicable		

Criteria C1.5	Compliance with the entity's confidentiality commitments and system requirements by vendors and other third parties whose products and services are part of the system is assessed on a periodic and as-needed basis and corrective action is taken, if necessary.	
QTS Description of control	**KPMG’s Test of controls**	**KPMG Results of tests**
C1.5.1 – As needed and as a part of the vendor and/or third party contract renewal, the QTS Legal Department initiates a review of the vendor and/or third party’s services to confirm that services are being provided per the contractual agreement and corrective action is taken as necessary.	Inspected a sample of new or amended contracts during the period to determine whether a review of the vendor and/or third party’s services took place to confirm that services are being provided per the contractual agreement and corrective action was taken as necessary.	No exceptions noted.
Complementary User Entity Controls: Not Applicable		

Criteria C1.6	Changes to entity's confidentiality commitments and system requirements are communicated to internal and external users, vendors, and other third parties whose products and services are part of the system.

QTS Description of control	KPMG's Test of controls	KPMG Results of tests
C1.6.1 – As needed, the QTS Legal Department communicates changes to confidentiality practices and commitments to internal users, through updates to formal processes, such as changes to standard contract language and confidentiality policies.	Inspected documentation for a sample of confidentiality practice and commitment changes to determine whether the changes are communicated to internal users through the updates to formal processes, such as changes to standard contract language and confidentiality policies.	No exceptions noted.
C1.6.2 – As needed, the QTS Legal Department communicates changes to confidentiality practices and commitments to external users, including vendors, and third parties through updates to formal processes, such as changes to standard contract language and confidentiality policies.	Inspected documentation for a sample of confidentiality practice and commitment changes to determine whether the changes are communicated to external users through the updates to formal processes, such as changes to standard contract language and confidentiality policies.	No exceptions noted.

Criteria C1.6	Changes to entity's confidentiality commitments and system requirements are communicated to internal and external users, vendors, and other third parties whose products and services are part of the system.	
QTS Description of control	**KPMG’s Test of controls**	**KPMG Results of tests**
C1.6.3 – QTS communicates to customers’ roles and responsibilities and security, availability, and confidentiality commitments within the Data Center handbook located on the Customer Portal. The Customer Portal lists the customer's responsibilities and process to report operational failures, incidents, problems, concerns and complaints.	Inspected QTS' customer portal to determine whether the data center handbook is available and customers' responsibilities, which include responsibility for reporting operational failures, incidents, problems, concerns and complaints, and the process for doing so, are also described in the customer portal. Inspected a sample of Data center handbooks to determine whether the entity’s security, availability, and confidentiality commitments, roles and responsibilities were included.	No exceptions noted.
Complementary User Entity Controls: Not Applicable		

Criteria C1.7	The entity retains confidential information to meet the entity's confidentiality commitments and system requirements.

QTS Description of control	KPMG's Test of controls	KPMG Results of tests
C1.7.1 – The QTS Operations Department securely retains confidential information in accordance with QTS retention standards unless otherwise stated within the customer service level agreement. Confidential information is disposed of after the retention period has expired.	Inspected the QTS retention standards and supporting documentation for a sample of backups containing confidential information to determine whether confidential information is retained and disposed of per the QTS retention standards unless otherwise stated within the customer service level agreement.	No exceptions noted.
C1.7.2 – As needed, the QTS Legal Department makes changes to confidentiality practices and commitments to reflect changes in business processes and requirements. Formal processes, such as changes to standard contract language and confidentiality policies, are used to communicate these changes to users, vendors, and third parties.	Inspected documentation for a sample of confidentiality practice and commitment changes to determine whether the changes are communicated to external users through the updates to formal processes, such as changes to standard contract language and confidentiality policies.	No exceptions noted.

Criteria C1.7	The entity retains confidential information to meet the entity's confidentiality commitments and system requirements.	
QTS Description of control	**KPMG's Test of controls**	**KPMG Results of tests**
C1.7.3 – The QTS Facilities Department securely retains log and video records of data center physical access events onsite for at least three months on a local database to allow for subsequent review of security events. Backups are also securely stored offsite for disaster recovery for the duration of the retention period.	Inspected sample log records and video records of data center access events from the in-scope facilities to determine that these are securely retained for at least three months locally, and securely stored offsite for disaster recovery for the duration of the retention period.	No exceptions noted.
Complementary User Entity Controls: Not Applicable		

Criteria C1.8	The entity disposes of confidential information to meet the entity’s confidentiality commitments and system requirements.

QTS Description of control	KPMG’s Test of controls	KPMG Results of tests
C1.8.1 – The QTS Operations Department securely retains confidential information in accordance with QTS retention standards unless otherwise stated within the customer service level agreement. Confidential information is disposed of after the retention period has expired.	Inspected the QTS retention standards and supporting documentation for a sample of backups containing confidential information to determine whether confidential information is retained and disposed of per the QTS retention standards unless otherwise stated within the customer service level agreement.	No exceptions noted.
C1.8.2 – As needed, the QTS Legal Department makes changes to confidentiality practices and commitments to reflect changes in business processes and requirements. Formal processes, such as changes to standard contract language and confidentiality policies, are used to communicate these changes to users, vendors, and third parties that dispose of confidential information.	Inspected documentation for a sample of confidentiality practice and commitment changes to determine whether the changes are communicated to internal and external users through the updates to formal processes, such as changes to standard contract language and confidentiality policies.	No exceptions noted.
Complementary User Entity Controls: Not Applicable		

Section V - Other information provided by QTS Realty, Inc. that is not covered by the service auditor's report

Additional QTS service lines

QTS provides a comprehensive suite of C3 – Cloud Services, Managed Services and Professional Services offerings, detailed in its Service Catalog, which have been designed to meet the needs of small, medium, and Fortune 500 companies across the globe. The scope of this report does not include C3 – Cloud Services, Managed Services or Professional Services as noted under Scope and Objectives in Section III.

Cloud services

QTS' cloud products provide virtualized solutions which offer IT infrastructure to support varied business application requirements. Cloud products include the same high-speed Internet connections, security systems and procedures, fully redundant power, cooling and environmental systems as the colocation solution. However, cloud products are in a virtualized environment which can be fully managed or self-managed to maximize utilization and cost-effectiveness across IT network, compute and storage resources. To meet customers' business and regulatory requirements, QTS has developed three cloud offerings:

- QTS Enterprise Cloud – Flexible, secure and scalable infrastructure as a service solution designed to meet the needs of today's Enterprise.
- QTS Federal Cloud – Highly secure, certified FedRAMP Cloud purpose built for federal government agencies.
- QTS DRaaS – Enterprise-grade disaster recovery offering that reduces complexity and minimizes risk.

Managed services

QTS offers a broad array of managed services, from a fully managed virtual infrastructure to a la carte networking, security, storage and backup, and disaster recovery services that can be added to your existing infrastructure. By leveraging the systems, processes and infrastructure deployed throughout the QTS' data centers, QTS can deliver flexible, highly customizable managed services solutions to our customers.

Managed hosting – Shared (QVI) and Dedicated (Custom)

Managed hosting is a bundled, fully managed virtualized hosted solution that provides inherent flexibility to maximize utilization and cost-effectiveness across customer network, compute and storage resources. In the custom dedicated model, customers can deploy dedicated or hybrid IT environments to support requirements of both cloud and legacy applications by selecting and bundling network and systems, security, storage and backup, disaster recovery, and 24x7x365 operations service center services. In the Shared QTS Virtualized Infrastructure (QVI) model, the computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

Managed Network

QTS offers managed network options. Network management expertise providing network availability, performance and visibility through management of network routers, Layer 2 and Layer 3 switches, firewalls, load balancers, virtual private networks, and border gateway protocols:

- Managed Switch – QTS Managed Switch is a fully managed service that includes monitoring, configuration reviews, customer change requests, software reviews, software updates, and ongoing management of supported Layer 2 Devices (these join multiple network devices together within one local area network (LAN) and capable of moving packets from one source to another based on the Mac address of the destination device).
- Managed Load Balancer – QTS Managed Load Balancing service includes a network device that accepts traffic on behalf of a group of servers, and distributes that traffic according to the load and availability of servers running on the individual servers. This service includes monitoring, configuration reviews, customer change requests, software reviews, software updates, and ongoing management of supported load balancer devices.
- Managed Firewall – QTS Managed Firewall is designed to block unauthorized access, while permitting authorized communications. The firewall can be configured to permit, deny, encrypt, or decrypt all computer traffic between different security networks based upon a set of ruled and other criteria. This service includes monitoring, configuration reviews, customer change requests, software reviews, software updates, and ongoing management of supported firewall devices.
  - A managed VPN connection, made using a QTS-managed firewall appliance, is included in QTS Managed Firewall. The firewall appliance encrypts traffic over the public internet to connect remote sites or users together. This service provides configuration, support, and ongoing management of site-to-site and customer-to-site (remote access) VPN.

Managed systems

QTS offers managed network and system options, for a variety of networking equipment and operating systems, under its QTS Managed Network, QTS Managed Operating Systems (OS) and QTS Managed Applications service lines:

- QTS Managed OS – Managed systems services including Operating Systems, Active Directory, and Distributed DNS Hosting. Supported operating systems include Windows®, UNIX/AIX™/Linux, and VMware® and includes base operating system management, updating and patching services. Active Directory services provide centralized account management, internal DNS capabilities and the domain structure required for cluster services. Distributed DNS Hosting services are also available, providing highly available, redundant and geographically distributed authoritative name servers built using BIND 9 technology.
- QTS Managed Servers – QTS Managed Server service delivers an array of features – server platform design and sizing, configuration, management, maintenance, support and reporting. The service is supported by the 24x7x365 monitoring systems.
- QTS Managed Applications – Provide services for application monitoring and testing, IIS (Internet Information Services) web server services, and DB system administration management. Monitoring and testing services provide comprehensive insight into system health as well as automatic notification of system events.
- QTS Managed Databases- QTS Managed Database service delivers an array of features – database platform design and sizing, configuration, management, maintenance, support and reporting. The service is supported by the 24x7x365 monitoring systems.

Monitoring Services

QTS Monitoring continuously tests customers' IT infrastructure elements (switches, firewall, servers, operating systems, and URLs) for availability and performance. For fully managed service elements, event alerts or alarms detected by QTS monitoring systems flow into the QTS OSC 24x7x365.

Security

QTS Managed Security is an integrated, fully managed cloud-based suite of security and compliance solutions for hybrid IT environments. The solution is comprised of QTS Network Intrusion Detection System (IDS), and QTS Log Management.

QTS Network Intrusion Detection System is a highly compliant, fully managed cloud-based vulnerability assessment and intrusion detection solution that allows customers to quickly identify and handle suspicious network traffic, and provides insights into threats and vulnerabilities. The solution is fully managed and supported by a 24x7x365 Security Operations Center (SOC), includes over 60,000 IDS threat signatures, real-time signature updates, and custom rule creation and editing, a vulnerability assessment and intrusion detection capability, and analysis and reporting.

QTS Log Management collects, aggregates, and normalizes log data, and provides a single view into customers IT Infrastructure. With flexible data collection options including agent only, physical, or virtual appliances with agent-based or agentless methodology, are available for customers' hybrid environments from colocation to cloud.

Managed Backup and Storage

QTS provides a portfolio of data storage and backup protection services to customers based on best of breed technologies. Services include:

- Managed Backup Shared – A comprehensive backup solution that runs on a private, secure, in-house network to store customer data on tape or disk. Utilizes industry leading Storage Tek and DATADomain hardware with Symantec NetBackup and Aptare software.
- Managed SAN – A fast, reliable, and scalable Fiber Channel and iSCSI SAN attached storage service. The platform is based on EMC, CLARiiOn, VNX, Brocade, Network Appliance, and Cisco technologies.
- SAN-to-SAN – A replication Shared providing a viable disaster recovery solution for existing managed SAN customers. The service provides block asynchronous replication of data between two of QTS' state-of-the-art data centers.
- Managed Tape Rotation – Manages the movement of customer data storage media to and from a secure off-site location.

Disaster Recovery Services

QTS provides a portfolio of flexible disaster recovery services to protect customer data and support their IT infrastructure's availability. Services include:

- Website Failover Service – Redirects customers DNS in the event of customers' primary server unavailability of underperformance.
- DR On-Demand – A cost-effective, image based, replication solution for virtual servers.
- DR High Availability Service – Continuous data replication for customers' physical and virtual servers.

Connectivity

QTS offers a full range of interconnection and IP bandwidth options that enable visionary flexibility into customers IT services. QTS Interconnection Services provide customers the ability to easily connect to the Internet, in-building carriers, or to an array of business partners within QTS data centers, or to hundreds of other network providers at the regional carrier hotels. Internet bandwidth services offer convenient, high-performance, bandwidth services utilizing the QTS carrier-neutral model of internet access options available at each data center.

Professional services

QTS' Professional Services organization assists customers with implementing appropriate technology solutions. Whether the customer is looking for design, development, implementation support or consulting, QTS' skilled professionals can assist the planning, build or integration efforts related to any of the following areas: data center migration, space utilization and power configuration, network design and architecture, backup and storage systems design and validation, security and access controls, systems and application configuration and interoperability, and program and project management. QTS' certified engineers and operations experts support QTS customer projects and help QTS customers maximize the performance and value of their infrastructure and data center operations.

Management's responses to exceptions noted

Criterion CC5.1 and CC6.1

The QTS Piscataway and Chicago sites are new sites within the QTS portfolio. QTS' Information Security Office (ISO) reviewed the best deployment and integration methods for the Intrusion Detection System, performing final deployment of the system on 7/20/2017. During the period 10/1/2016 to 7/19/2017, the ISO relied on other mitigating controls for potential breach identification and detection methods including:

- Infrastructure systems & networking monitoring and event log reviews
- Physical Security and Data Center Operations personnel daily system interaction
- Centrally managed Symantec end point protection solution with event notification and reporting
- Internal and external incident reporting and response procedures

Additionally, ISO performed external vulnerability scanning of the locations DMZ to identify, detect, and remediate potential breach vulnerabilities.

Criterion CC1.4

Management acknowledges there was a miss in an employee to get a signature on non-disclosure agreement (NDA) and/or confidentiality agreements (CA) within ten (10) calendar days of employment. QTS has in place the following controls that will mitigate the impact of this exception:

- We have created one template for a couple of New Hire documents (Confidentiality and Non solicitation agreement, federal state tax form, direct deposit authorization, emergency contact information form, EEO self Id form, Conflict of Interest) to ensure they are all sent together and received together as one document.
- We do not clear the candidate to start employment till we receive the New Hires template duly signed from them.